**INTERNATIONAL SCHOOL OF   
MANAGEMENT AND TECHNOLOGY**



**FACULTY OF COMPUTING**

**ASSIGNMENT COVER SHEET**

*This form is to be completed by students submitting assignments of level 4 and level 5. Students are required to complete all sections and attach to your assignment.*

|  |  |
| --- | --- |
| STUDENT DETAILS | |
| STUDENT NAME | Dipak Shah |
| STUDENT ID |  |

|  |  |  |  |
| --- | --- | --- | --- |
| UNIT AND ASSIGNMENT DETAILS | | | |
| UNIT TITLE | Cloud Computing | | |
| UNIT NUMBER | F/615/1644 | | |
| ASSIGNMENT TITLE | Siddhartha Cloud Computing Pvt. | | |
| ISSUE DATE | 29/09/2023 | DUE DATE | 28/11/2023 |
| ASSESSOR NAME | Siddhant Bhattarai | | |
| ESTIMATED WORD LENGTH |  | | |

|  |  |
| --- | --- |
| SUBMISSION | |
| HAND IN DATE | 11/22/2023 |

**DECLERATION AND ACKNOWLEDGEMENT**

***When submitting assignments, each student must sign a declaration confirming that the work is their own.***

*Plagiarism and Collusion*

**Plagiarism:** to use or pass off as one’s own, the writings or ideas of another without acknowledging or crediting the source from which the ideas are taken.

**Collusion:** submitting an assignment, project or report completed by another person and passing it off as one’s.

In accordance with the*Academic Integrity and Plagiarism Policy*:

1. **I declare that:**
2. this assignment is entirely my own work, except where I have included fully-documented references to the work of others,
3. the material contained in this assignment has not previously been submitted for any other subject at the University or any other educational institution, except as otherwise permitted,
4. no part of this assignment or product has been submitted by me in another (previous or current) assessment, except where appropriately referenced, and with prior permission from the Lecturer / Tutor / Unit Coordinator for this unit.
5. **I acknowledge that:**
6. if required to do so, I will provide an electronic copy of this assignment to the assessor;
7. the assessor of this assignment may, for the purpose of assessing this assignment:
8. reproduce this assignment and provide a copy to another member of academic staff;
9. communicate a copy of this assignment to a plagiarism checking service such as Plagiarism Check (which may then retain a copy of this assignment on its database for the purpose of future plagiarism checking).

|  |  |  |  |
| --- | --- | --- | --- |
| I am aware of and understand that any breaches to the Academic Code of Conduct will be investigated and sanctioned in accordance with the College Policy. | | | |
| SIGNATURE | Dipak | DATE | 11/22/2023 |

Table of Contents

[Introduction 10](#_Toc152070816)

[What is cloud computing? 10](#_Toc152070817)

[Impact of Cloud Computing 10](#_Toc152070818)

[Background 11](#_Toc152070819)

[Purpose of report 11](#_Toc152070820)

[Scope 11](#_Toc152070821)

[Objectives 11](#_Toc152070822)

[Analyzes the evolution and fundamental concept of cloud computing: 11](#_Toc152070823)

[Traditional Networking (Pre-Cloud Era): 12](#_Toc152070824)

[Client-Server Architecture (1980s-1990s): 12](#_Toc152070825)

[Virtualization (Late 1990s-2000s): 12](#_Toc152070826)

[Utility Computing and the Birth of Cloud (Mid-2000s): 12](#_Toc152070827)

[Service-Oriented Architecture (SOA): 13](#_Toc152070828)

[Ubiquitous Computing (Present-Day): 13](#_Toc152070829)

[Key concept of cloud computing 13](#_Toc152070830)

[1. Service model 13](#_Toc152070831)

[a. Infrastructure as a Service (IaaS): 14](#_Toc152070832)

[Features 14](#_Toc152070833)

[Use case 14](#_Toc152070834)

[b. Platform as a Service (PaaS): 14](#_Toc152070835)

[Features 14](#_Toc152070836)

[Use case 15](#_Toc152070837)

[c. Software as a Service (SaaS): 15](#_Toc152070838)

[Features 15](#_Toc152070839)

[Use case 15](#_Toc152070840)

[2. Development model 15](#_Toc152070841)

[a. Public cloud 15](#_Toc152070842)

[i. Use 16](#_Toc152070843)

[b. Private cloud 16](#_Toc152070844)

[i. Use 16](#_Toc152070845)

[c. Hybrid cloud 16](#_Toc152070846)

[i. Use 16](#_Toc152070847)

[Benefits of Cloud Computing 17](#_Toc152070848)

[ Flexible Resource Allocation: 17](#_Toc152070849)

[ Cost-effectiveness: 17](#_Toc152070850)

[ Global access: 17](#_Toc152070851)

[ Security: 18](#_Toc152070852)

[ Insight: 18](#_Toc152070853)

[ Increased Collaboration: 18](#_Toc152070854)

[ Quality Control: 18](#_Toc152070855)

[ Disaster Recovery: 19](#_Toc152070856)

[ Loss Prevention: 19](#_Toc152070857)

[ Automatic Software Updates: 19](#_Toc152070858)

[ Competitive Edge: 19](#_Toc152070859)

[ Sustainability: 20](#_Toc152070860)

[Disadvantage 20](#_Toc152070861)

[ Data Security: 20](#_Toc152070862)

[ Automated Service provisioning: 20](#_Toc152070863)

[ Virtual machine migration: 20](#_Toc152070864)

[ Energy management: 21](#_Toc152070865)

[ Traffic management and analysis: 21](#_Toc152070866)

[ Constant network connection: 21](#_Toc152070867)

[ Generic: 21](#_Toc152070868)

[Architectural Framework Design 22](#_Toc152070869)

[Components of the Proposed Framework 23](#_Toc152070870)

[Scalability and Redundancy Considerations 25](#_Toc152070871)

[Redundancy Strategies: 26](#_Toc152070872)

[Defines an appropriate deployment model and compares the service models for choosing a model for the London College: 27](#_Toc152070873)

[Private Cloud: 27](#_Toc152070874)

[Public Cloud: 28](#_Toc152070875)

[Community Cloud: 28](#_Toc152070876)

[Hybrid Cloud: 28](#_Toc152070877)

[Comparing Service Models: 28](#_Toc152070878)

[Choosing the Most Suitable Model for the London College: 29](#_Toc152070879)

[Demonstration of Selected Deployment Models with Real-World Examples: 29](#_Toc152070880)

[Selection of hybrid cloud for London collage 31](#_Toc152070881)

[Benefits of selecting hybrid model 31](#_Toc152070882)

[Examining Different Service Models 32](#_Toc152070883)

[1. Infrastructure-As-A-Service (IAAS) 32](#_Toc152070884)

[2. Platform-as-a-Service (PAAS) 33](#_Toc152070885)

[3. Software-As-A-Service (SaaS) 33](#_Toc152070886)

[Selecting the Right Service Model for The London College 34](#_Toc152070887)

[Compelling Reasons for Cloud Migration 34](#_Toc152070888)

[Advantages of Migrating to a Cloud Computing Solution 35](#_Toc152070889)

[ Flexibility and Scalability: 36](#_Toc152070890)

[ Cost Efficiency: 36](#_Toc152070891)

[ Enhanced Accessibility and Collaboration: 36](#_Toc152070892)

[ Simplified Maintenance and Management: 36](#_Toc152070893)

[ Business Continuity and Disaster Recovery: 36](#_Toc152070894)

[ Technological Advancements and Innovation: 36](#_Toc152070895)

[ Robust Security and Compliance: 36](#_Toc152070896)

[Demonstrating Deployment Models 37](#_Toc152070897)

[Public cloud 37](#_Toc152070898)

[AWS Elastic Beanstalk (EBS) 37](#_Toc152070899)

[Illustrating Public Cloud Deployment 37](#_Toc152070900)

[7.2 Showcasing Private Cloud Deployment 40](#_Toc152070902)

[Code used in process 41](#_Toc152070903)

[Highlighting Hybrid Cloud Scenarios 45](#_Toc152070904)

[Justification for Tool Selection 46](#_Toc152070905)

[Migrating the London College's IT Services (Theoretical Process) 48](#_Toc152070906)

[Configuring Auto-Scaling Groups for EC2 Instances: 49](#_Toc152070907)

[Implementing an Application Load Balancer: 49](#_Toc152070908)

[Enabling Auto Scaling for Dynamic Resource Management: 49](#_Toc152070909)

[Conclusion 50](#_Toc152070910)

[Part-2 50](#_Toc152070911)

[Introduction 50](#_Toc152070912)

[Purpose of the Report 50](#_Toc152070913)

[Scope and Objectives 50](#_Toc152070914)

[Overview of Cloud Computing Solutions 51](#_Toc152070915)

[Implementing a Cloud Computing Platform using Open-Source Tools 98](#_Toc152070931)

[Selection of Open-Source Tools and Technologies 98](#_Toc152070932)

[Potential Issues and Constraints 99](#_Toc152070933)

[Network Latency and Performance Challenges 99](#_Toc152070934)

[Data Security and Compliance Concerns 99](#_Toc152070935)

[Cost Management and Budget Constraints 99](#_Toc152070936)

[Training and Skill Gaps among IT Staff 100](#_Toc152070937)

[Vendor Lock-In and Portability Issues 100](#_Toc152070938)

[Network Latency and Performance Challenges 100](#_Toc152070939)

[Challenges Related to Network Latency and Performance 100](#_Toc152070940)

[Addressing Data Security and Compliance Concerns 101](#_Toc152070941)

[Managing Costs in Alignment with Budget Constraints 101](#_Toc152070942)

[Training and Skill Development Initiatives 101](#_Toc152070943)

[Vendor Lock-In and Portability Issues 102](#_Toc152070944)

[Conclusion 102](#_Toc152070945)

[Part-3 102](#_Toc152070946)

[Introduction 102](#_Toc152070947)

[Purpose of article 103](#_Toc152070948)

[Scope of article 103](#_Toc152070949)

[Common Problems in Cloud Computing 103](#_Toc152070950)

[ Scalability Challenges 104](#_Toc152070951)

[ Data Loss and Recovery 104](#_Toc152070952)

[ Cost Management and Overspending 104](#_Toc152070953)

[ Vendor Lock-In and Portability 104](#_Toc152070954)

[ The Most Common Cloud Computing Problems and their Solutions 105](#_Toc152070955)

[Contemporary Security Issues in the Cloud 105](#_Toc152070956)

[ Data Breaches and Unauthorized Access 105](#_Toc152070957)

[ Data loose 106](#_Toc152070958)

[ Inadequate Identity and Access Management 106](#_Toc152070959)

[ Insider Threats and Data Leakage 106](#_Toc152070960)

[ Strategies for Addressing Current Cloud Security Issues: 106](#_Toc152070961)

[Building a Secured Cloud Computing Platform 106](#_Toc152070962)

[ Identity and Access Management Best Practices 107](#_Toc152070963)

[ Data Encryption and Tokenization 107](#_Toc152070964)

[ Continuous Monitoring and Threat Detection 107](#_Toc152070965)

[ Compliance and Auditing Solutions 107](#_Toc152070966)

[ Employee Training and Security Awareness 107](#_Toc152070967)

[Data Protection During Cloud Migration 108](#_Toc152070968)

[ Understanding Data Classification and Sensitivity 108](#_Toc152070969)

[ Data Encryption and Secure Transfer 108](#_Toc152070970)

[ Backup and Disaster Recovery Planning 109](#_Toc152070971)

[ Legal and Regulatory Compliance 109](#_Toc152070972)

[ Creating a Data Protection Strategy for the London College. 109](#_Toc152070973)

[Conclusion 109](#_Toc152070974)

[Reference 111](#_Toc152070975)

[Figure 1 3-tire model 23](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071461)

[Figure 2 EBS\_LAB\_1 37](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071462)

[Figure 3 checking environment is fine or not 38](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071463)

[Figure 4 selecting environment 38](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071464)

[Figure 5 updated successfully 39](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071465)

[Figure 6 uploading tomcat.zip file 39](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071466)

[Figure 7 final part 40](#_Toc152071467)

[Figure 8 logging to private cloud 40](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071468)

[Figure 9 Linux dashboard 41](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071469)

[Figure 10 code to run website 43](#_Toc152071470)

[Figure 11 London collage website 45](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071471)

[Figure 12 creating VPC 52](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071472)

[Figure 13 VPC created successfully 53](#_Toc152071473)

[Figure 14 creating subnet 53](#_Toc152071474)

[Figure 15 created all six subnet 57](#_Toc152071475)

[Figure 16 creating internet gateway 58](#_Toc152071476)

[Figure 17 internet gateway created successfully 58](#_Toc152071477)

[Figure 18 Attach VPC in internet gateway 59](#_Toc152071478)

[Figure 19 Created two NAT gateway successfully 62](#_Toc152071479)

[Figure 20 creating public route table 63](#_Toc152071480)

[Figure 21 Adding subnet into route table 64](#_Toc152071481)

[Figure 22 editing route table and adding internet gateway 64](#_Toc152071482)

[Figure 23 complete route table 65](#_Toc152071483)

[Figure 24 creating private route table 66](#_Toc152071484)

[Figure 25 Adding NAT gateway 67](#_Toc152071485)

[Figure 26 creating second private route table 69](#_Toc152071486)

[Figure 27 creating EC2 71](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071487)

[Figure 28 Creating key-pair 72](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071488)

[Figure 29 adding security 73](#_Toc152071489)

[Figure 30 EC2 created successfully 73](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071490)

[Figure 31 running from DNS 74](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071491)

[Figure 32 using codes 76](#_Toc152071492)

[Figure 33 London college websites 79](#_Toc152071493)

[Figure 34 Creating image 79](file:///E:\Cloud%20computing\Assignment%20C.C.docx#_Toc152071494)

[Figure 35 selecting instances 79](#_Toc152071495)

[Figure 36 adding target group 80](#_Toc152071496)

[Figure 37 selecting VPC 81](#_Toc152071497)

[Figure 38 creating target group 81](#_Toc152071498)

[Figure 39 creating Application Load Balancer 82](#_Toc152071499)

[Figure 40 selecting zones 82](#_Toc152071500)

[Figure 41 selecting target group 83](#_Toc152071501)

[Figure 42 summary of load balancer 84](#_Toc152071502)

[Figure 43 created load balancer successfully 84](#_Toc152071503)

[Figure 44 now creating launch template 85](#_Toc152071504)

[Figure 45 enable cloud monitor 88](#_Toc152071505)

[Figure 46 created load balancer successfully 88](#_Toc152071506)

[Figure 47 selecting lunch template 89](#_Toc152071507)

[Figure 48 creating auto scaling groups 90](#_Toc152071508)

[Figure 49 adding load balancing 91](#_Toc152071509)

[Figure 50 creating capacity 93](#_Toc152071510)

[Figure 51 review everything and creating auto scaling 96](#_Toc152071511)

[Figure 52 created auto scaling 96](#_Toc152071512)

[Figure 53 Copy DNS name to run cloud watch 97](#_Toc152071513)

[Figure 54 running website 97](#_Toc152071514)

[Figure 55 current CPU load 97](#_Toc152071515)

# Introduction

The London College is undergoing a considerable transition in order to adapt to the ever-changing world of technology. They are transitioning from traditional on-premises servers to more flexible cloud-based solutions. This paper will provide an overview of the migration decision, explain why Siddhartha Cloud Computing Pvt. Ltd. was selected as the service provider, and discuss the full migration plan to Amazon Web Services (AWS). This study intends to be a helpful guide, shining light on the migration's reasoning, tools and architecture used, and solutions applied to enable a seamless and effective transition.

# What is cloud computing?

Cloud computing is a model of providing access to servers, storage, databases, networks, software, analysis etc., through the cloud rather than using physical computers or local infrastructure. It allows users can be able to access and use computing resources as necessary, many times, paying for it according to usage or subscription based.

# Impact of Cloud Computing

The area of technology and business operations has undergone a significant transformation with the advent of cloud computing. It has multidimensional implications in the domain of IT infrastructure and its influence on how an organization operates. Scalability and flexibility are some of its notable effects that enable organizations to adjust their resources as much as required according to varying demand. This elasticity helps in lowering costs as well as streamlining operations because a company pays for the used resources. This has made it possible for remote access of data and applications, increasing global connection and world-wide cooperation which are no more restricted to a particular place as they were before. In addition, cloud computing has boosted innovation enabling quick adoption of advancement including artificial intelligence, data science, and machine learning. This is vital, enabling fast provisioning of new applications and products that drives innovation for organizations operating under tight competition scenarios. Also, the cloud’s strong business continuity solutions and data protection are key factors in today’s world. In summary, cloud computing is more of an evolutionary process and not just a simple technology advancement. It constitutes a revolutionary stride that enables organizations to be flexible, creative, and globally connected for survival in this digitally oriented world.

# Background

The London College, an institution currently reliant on on-premises servers for hosting its services, has made a strategic decision to transition its operations to the cloud. To facilitate this migration, Siddhartha Cloud Computing Pvt. Ltd., based in Kathmandu, Nepal, has been engaged. The rationale behind this shift is rooted in the college’s pursuit of enhanced scalability, improved a Cloud Computing feasibility, fortified reliability, and bolstered security measures.

# Purpose of report

The purpose of this report is to document the procedures that were followed to migrate all of The London College's data and services—including its website—to the AWS Cloud. It will describe the tactics, resources, and procedures employed in this process, emphasizing the technical aspects and providing justification for the choices taken. It will also go over the particular duties required, the objectives, and the recommended fixes to guarantee as a Cloud Computing and seamless move.

# Scope

* Migration of The London College's on-premises services to the AWS Cloud.
* Emphasis on the hosting of the college website and the complete transfer of associated data.
* Consideration of challenges, tools, and methodologies employed throughout the migration.

# Objectives

* Analysis of the evolution and fundamental concepts of cloud computing.
* Justification of the migration from on-premises servers to the cloud.
* Rationale behind the selection of tools and frameworks for the cloud migration.
* Design of an appropriate cloud computing architecture for The London College.
* Development and implementation of cloud computing solutions using AWS frameworks and open-source tools.
* Addressing issues, constraints, and strategies to overcome challenges during the migration process.

Analyzes the evolution and fundamental concept of cloud computing:

This means IT resources such as computing power and storage are available on cloud computing a technology model offered over the internet. You instead rent computing space off cloud services such as those provided by AWS. It’s like paying for computing power only when you need it, not buying and supporting it. A lot has changed in cloud computing starting back when it was introduced, especially growing with additional technologies and varying business needs. Here's a breakdown of how cloud computing has changed over time and the essential ideas it's built upon:

# Traditional Networking (Pre-Cloud Era):

In the pre-cloud era, computing primarily relied on traditional networking and on-premises infrastructure. Organizations managed their own data centers, consisting of physical servers, storage systems, and networking equipment. These data centers were expensive to build and maintain, often leading to over-provisioning to a Cloud Computing peak loads. Scaling infrastructure required significant time and resources, and disaster recovery was challenging.

# Client-Server Architecture (1980s-1990s):

The shift to client-server architecture marked a significant departure from the mainframe era. Organizations built networks of interconnected servers and client machines, allowing for distributed computing. While this improved resource sharing and reduced centralization, it still relied on on-premises infrastructure and lacked the flexibility and scalability seen in modern cloud computing.

# Virtualization (Late 1990s-2000s):

The advent of such virtualization technologies was a game changer. It enabled the decoupling of software from hardware whereby multiple VMs could run on a single physical server. This innovation enabled improved hardware utilization at low costs and made infrastructure management and scaling simpler. While these were virtualized environments in some ways these were still on-premises.

# Utility Computing and the Birth of Cloud (Mid-2000s):

The mid-2000s witnessed the emergence of utility computing models. Amazon Web Services (AWS) played a pivotal role by introducing Elastic Compute Cloud (EC2) in 2006, allowing users to rent virtual servers on-demand. This marked the birth of cloud computing as we know it today. Cloud providers began offering Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) solutions, reducing the need for organizations to invest heavily in physical infrastructure.

# Service-Oriented Architecture (SOA):

Cloud computing was complemented by SOA. Through SOA, applications are further broken down into smaller, interchangeable components such as services which can be located and scaled independently on the cloud infrastructure. This modular way made it flexible, agile and easy to maintain – fit well within the cloud’s capability.

# Ubiquitous Computing (Present-Day):

Due to the widespread availability of internet connections, smartphones, and fast networks, cloud computing is now everywhere. The convenience with which people can use cloud services from anywhere, anytime, and on various devices has opened up technology to everyone. This widespread availability has greatly influenced the way company’s offer services and establish connections with their cliеntеlе.

# Key concept of cloud computing

To really unlock the full potential of cloud computing, you have to understand the basics. Lucky for you, this article does just that. By going over key concepts in cloud computing, this will give you a good foundation to build on with your knowledge. Different models and guiding concepts all make up the basic principles, which is what every other thing was built off. The section teaches important things like various services (such as SaaS, PaaS, and IaaS), essential features (like resource pooling and scalability), deployment models and even cost-effectiveness. This information is crucial for anyone looking to comprehend cloud computing and apply it suCloud Computing fully in different situations and Service model. There are different key concept of cloud computing such as:

# Service model

A service model in cloud computing denotes the type of service being offered by a cloud service provider. These refer to the models that govern various layers of the computing stack for the sake of supplying them to the end-users. There are primarily three main service models: IaaS, PaaS and SaaS.

# Infrastructure as a Service (IaaS):

Within the Infrastructure as a Service (Iaas), the virtual-computing resources are provided by the cloud provider through the internet. These include operating systems, networks, storage, virtual machines etc.

# Features

* The operating systems and apps that are installed on the infrastructure are controlled by the users.
* On-demand, scalable resources with pay-per-use pricing.
* Provides flexibility and does away with the requirement for physical hardware upkeep.

# Use case

The London College could use IaaS to host their applications and services on virtual servers provided by the cloud service provider, allowing for flexibility and scalability without managing physical servers.

# Platform as a Service (PaaS):

PaaS is one type of service model based on cloud computing which gives a flexible, scalable cloud platform for developing, running, and managing applications. It saves developers effort in installing updating applications and updates as well as hardware and eliminates all sorts of associated problems. In contrast, a third-party service provider delivers the entire PaaS environment or platform through the cloud.

# Features

* Streamlines the software development process.
* Offers development tools and pre-configured environments.
* Developers focus on coding and deploying applications without managing the underlying infrastructure.

# Use case

By using PaaS, London College may create and implement unique learning programs more quickly by avoiding having to worry about the supporting infrastructure.

# Software as a Service (SaaS):

Software is delivered via the internet by SaaS. Because the program is hosted and maintained centrally by the provider, users can a Cloud Computing and utilize it without installing or maintaining it themselves.

# Features

* Applications a Cloud Computing ensile via web browsers.
* No installation or maintenance required.
* Users pay for a subscription or usage basis.

# Use case

London College might use software as a service (SaaS) to a Cloud Computing web programs including productivity software, email, and learning management systems without having to worry about maintaining the software infrastructure.

# Development model

The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN. There are different types of development model, they are:

# Public cloud

A public cloud is a pool of virtual resources developed from hardware owned and managed by a third-party company that is automatically provisioned and allocated among multiple clients through a self-service interface. It’s a straightforward way to scale out workloads that experience unexpected demand fluctuations.

# Use

The London College might think about using a public cloud for jobs or services that don't involve really private data and don't need super strict control over information. They can use public cloud services from big companies like AWS, Azure, or GCP, which offer flexible resources and cost-effective solutions. This helps the college get affordable and scalable computing power for tasks that don't need strict data handling.

# Private cloud

A private cloud is a cloud computing environment dedicated to a single organization. Any cloud infrastructure has underlying compute resources like CPU and storage that you provision on demand through a self-service portal. In a private cloud, all resources are isolated and in the control of one organization.

# Use

A private cloud could be appropriate for sensitive data, such as student records or internal administration systems, to preserve strict control and ensure compliance. For increased protection, the college could host vital activities and sensitive data on a private cloud.

# Hybrid cloud

Hybrid clouds are more sophisticated than other deployment methods since they combine two or more clouds (private, communal, or public). Each member maintains a distinct entity, but is linked to others by standardized or proprietary technology that allows application and data transfer between them.

# Use

A hybrid cloud solution could be advantageous given the need for both flexibility and security. The London College may employ a mix of public and private clouds, allowing them to preserve sensitive data in the private cloud while using the public cloud for less sensitive applications or extra resources during peak demand.

# Benefits of Cloud Computing

Literature relevant to this study indicates that the potential benefits from the cloud based models are perceived to be the main cause behind the organizations' appetite for adopting Cloud Computing. Potential benefits can be outlined as significantly lower initial costs improved standardization of services. Improved scalability as well as a Cloud Computing sensibility, which has resulted in Cloud Computing being implemented across a number of sectors. Another advantage of Cloud Computing is that there are minimal requirements for the provision of Resources and maintenance after implementation. As a result, the implementing organization can concentrate more on its core business activities, Moreover, Cloud Computing can minimize the costs of infrastructure and platforms, increase network security and service scalability and improve speed of adoption, which are all key benefits in relation to e-government services. Furthermore, Cloud Computing is viewed as utility computing as its price will be charged dependent upon use. Regarding environmental concerns, the CLOUD COMPUTING model is viewed favorably. There are different benefits of Cloud Computing and each of these benefits will be explored in the following paragraphs:

# Flexible Resource Allocation:

Cloud services enable consumers to easily and quickly expand or decrease resources as needed. Because of this adaptability, firms could quickly adjust to changing customer needs without major upfront costs.

# Cost-effectiveness:

Pay as you go pricing for cloud computing allows consumers to only pay for the resources they really need. They are spared from having to make large initial investments in infrastructure and physical hardware. By giving the cloud service provider responsibility for management and upkeep, it also lowers operating expenses.

# Global access:

Cloud services available from anywhere with internet connection, supporting remote work and teamwork. This accessibility allows for global reach, enable smooth communication and collaboration among teams in different locations.

# Security:

Many organizations have security concerns when it comes to adopting a cloud-computing solution. After all, when files, programs, and other data aren't kept securely onsite, how can you know that they are being protected? If you can remotely access your data, then what's stopping a cybercriminal from doing the same thing? Well, quite a bit, actually.

# Insight:

As we move ever further into the digital age, it's becoming clearer and clearer that the old adage “knowledge is power” has taken on the more modern and accurate form: “Data is money.” Hidden within the millions of bits of data that surround your customer transactions and business process are nuggets of invaluable, actionable information just waiting to be identified and acted upon. Of course, sifting through that data to find these kernels can be very difficult, unless you have access to the right cloud-computing solution.

# Increased Collaboration:

If your business has two employees or more, then you should be making collaboration a top priority. After all, there isn't much point to having a team if it is unable to work like a team. Cloud computing makes collaboration a simple process. Team members can view and share information easily and securely across a cloud-based platform. Some cloud-based services even provide collaborative social spaces to connect employees across your organization, therefore increasing interest and engagement. Collaboration may be possible without a cloud-computing solution, but it will never be as easy, nor as effective.

# Quality Control:

Few things are as damaging to a company's performance as low-quality reports that are inconsistent. In a cloud-based system, all documents are saved in a single location and format. With everyone having access to the same knowledge, you can maintain data consistency, avoid errors by humans, and keep a record of any edits or updates. Managing information in silos, on the other hand, can result in employees accidentally saving different versions of documents, resulting in confusion and diluted data.

# Disaster Recovery:

Control is an issue that affects most successful businesses. It is disappointing because no matter how tightly controlled you might think you know your organization's processes, at some point or another there will always be certain factors that are just beyond the scope of your ability to control; and in today’s world, even just one minute worth of waste can translate In your services, downtime equates into losses in productiveness, revenue, as well as your company’s reputation.

# Loss Prevention:

If your organization isn't investing in a cloud-computing solution, then all of your valuable data is inseparably tied to the office computers it resides in. This may not seem like a problem, but the reality is that if your local hardware experiences a problem, you might end up permanently losing your data. This is a more common problem than you might realize computers can malfunction for many reasons, from viral infections, to age-related hardware deterioration, to simple user error. Or, despite the best of intentions, they can be misplaced or stolen (over 10,000 laptops are reported lost every week at major airports).

# Automatic Software Updates:

For those who have a lot to get done, there isn't anything more irritating than having to wait for system updates to be installed. Cloud-based applications automatically refresh and update themselves, instead of forcing an IT department to perform a manual organization-wide update. This saves valuable IT staff time and money spent on outside IT consultation. PC World lists that 50% of cloud adopters cited requiring fewer internal IT resources as a cloud benefit.

# Competitive Edge:

Although cloud computing continues gaining more acceptance, some prefer to maintain everything within their local networks. It is their choice but they are incomparable with organizations that can use cloud facilities at their disposal. By implementing a cloud based solution ahead of your competitors you will have already learned enough to get an extra edge on them when they do catch up. The most recent Verizon survey revealed that about 77% of companies consider that using cloud technologies makes them more competitive; while 16% regard the advantage as really big.

# Sustainability:

In this context, putting a recycling bin into the breakroom is not sufficient to say that an organization cares about the planet. Real sustainable initiatives target needless wastage from every aspect of an organization. Cloud hosting is friendlier to the environment and has fewer carbon footprints.**”**

# Disadvantage

# Data Security:

Data security is a very relevant research topic in the field of challenges in shifting towards cloud computing. In cloud computing, organizations do not have direct control over their data that is stored in the cloud as they would have if it would have been stored in their own physical data centers. This could be a huge problem if we're dealing with really sensitive data. This puts the whole control in the hands of infrastructure providers to ensure data security using various security mechanisms.

# Automated Service provisioning:

Cloud holds the ability to provide its users to call for and also release resources on demand. In this case, the service provider is responsible. For allocating the required resources and de-allocating them when they've done their work. It is done to satisfy Service Level Objectives (SLOS) and also simultaneously reduce cost. But, it is not easy to map these SLOS with the requirements of the user in a timely manner especially when the requirements are low-level like CPU and memory requirements.

# Virtual machine migration:

Virtualization provides many benefits to cloud computing as it helps with balancing the load among data centers. However, providing these benefits are not as straightforward. For e.g. one of the benefits of virtualization is avoiding hotspots but it isn't straightforward, as loading virtual environment migrations do not deal well with continuous changes in the workload.

# Energy management:

Improving energy efficiency is one of the major challenges in cloud computing. This means cloud need to adhere to the environmental standards for the amount of energy being used. It is also a very costly matter. Powering and cooling the systems which provide the cloud. Services is a very costly affair and increase the expenditure on the companies' budget marginally. Not only money but also this is not a sustainable way of computing due to the huge amounts of energy being consumed. Therefore, there is huge pressure on the industry to reduce energy consumption brought on by the trend of cloud computing.

# Traffic management and analysis:

One thing that cloud providers provide their users is the detailed analysis of their data stored in the cloud. This helps them to see and analyses the trends and then create a customized report. This kind of analysis is really imperative for the companies, as it helps them with growing their business. But there aren't effective methods present which could help with providing a detailed analysis and the present methods cannot deal with thousands of different servers. So, traffic management and analysis remain a huge concern.

# Constant network connection:

Even though the user can access their data stored on the cloud from anywhere in the cloud, but it will only work if the user has constant access to a network connection. Also, cloud applications' performance would be directly dependent on the client's network connection. Since everything is online, speeds for downloading and uploading would be lower as compared to that of a local server.

# Generic:

Services provided by a public cloud provider are very generic. Not all organizations are comfortable with that. Trying to implement additional offerings can be a huge burden on smaller companies, as it requires a lot of internal resources.

# Architectural Framework Design

Understanding The London College's cloud migration project requirements are a vital step in ensuring a smooth transition. This procedure includes a thorough examination of the college's current environment, applications, and data. It entails determining which apps are mission-critical and require relocation, as well as mapping dependencies between programs and the data they contain. Furthermore, it is critical to analyze performance and workload trends to ensure that the cloud solution can fulfill the college's performance requirements, even during peak usage periods.

Additionally, it's crucial to prioritize security and compliance. It's important to recognize sensitive data and put in place strong security measures to safeguard information about students and staff. The college's compliance needs, determined by industry or legal standards, should also be part of the migration plan. Knowing how much the system needs to grow and being ready for changes in how much resources are needed is important. This way, resources can be adjusted as required to handle different workloads.

Finally, keeping costs in check is a big concern, so it's crucial to carefully analyze the budget to manage expenses effectively. Checking the current on-site systems and how they're linked will help make the move to the cloud smoother and ensure everything works well together. Knowing what the end-users—students, faculty, and staff—expect is really important to give them a seamless experience. Also, it's essential to train the staff and have strategies for managing changes to make sure everyone at the college can work well in the new cloud setup. This clear understanding of what's needed is the basis for Siddhartha Cloud Computing Pvt. Ltd. to create a tailor-made plan for moving to the cloud that perfectly fits The London College's specific needs and goals.

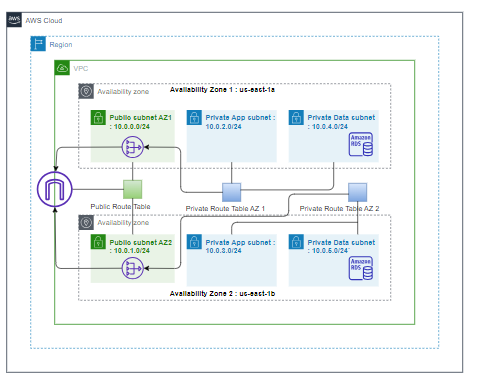


Figure 1 3-tire model

# Components of the Proposed Framework

The suggested cloud computing framework includes crucial components to ensure a stable and personalized cloud architecture in the context of moving The London College's services to AWS. These essential components are as follows:

* Amazon EC2 instances: The Elastic Load Balancing service provided by AWS facilitates traffic distribution to EC2 instances across multiple available sources and zones, allowing for the dynamic addition and removal of Amazon EC2 hosts from the load-balancing rotation.
* Amazon S3 (Simple Storage Service): Amazon S3 Standard provides high durability, performance and availability object storage for data that are frequently accessed. Due to its high throughput and low latency, Standard is perfectly suited for cloud applications, dynamic websites, mobile applications, gaming applications, big data analytics and content distribution. Policies are configured, by lifecycle management, for objects migration to appropriate storage class.
* Amazon RDS (Relational Database Service): Amazon’s MySQL RDS offering provides an implementation of MySQL on a virtual operating system.
* Amazon VPC (Virtual Private Cloud): Virtual private cloud (VPC) is a private network within public cloud infrastructure. It offers multiple users with the provision of private, isolated section of cloud infrastructure where the user can launch resources on-demand in a virtual network that they define. Using a public cloud environment gives businesses the flexibility and benefits of a cloud, such as scalability and reduced IT costs. Adding a private network within the public cloud
* AWS Auto Scaling: Auto scaling technique provides on-demand resources availability based on certain workloads in cloud computing systems. The Auto scaling service allows the configuration of capacity management policies applied to dynamically decide on acquiring or releasing resource instances for a given application.
* Elastic Load Balancing (ELB): Load Balancing is a technique to redistribute the load across the nodes. The decision to balance load is made locally by a node, based on its current utilization. Each node continuously measures its resource utilization of CPU, memory, network consumption and disk space
* AWS IAM (Identity and Access Management): In contrast to traditional XML (or JSON in case of AWS IAM) based authorization policy specification languages, our approach is formal and based on Event-Calculus, a logical language for specification of and reasoning about events and their effects. We have applied our approach to model and verify AWS IAM policies. We have categorized conflicts as either Intra or Inter-Policy conflicts. To best of our knowledge there exists no approach that attempts to model and verify IAM policies.
* Encryption Services: There are other ways to prevent hackers from damaging the system after hacking into an AWS account. For example, encrypting data information in the AWS cloud. There are many different encryption service providers in the AWS marketplaces, such as Safe Net and Vormetric, can provide a variety of encryption services. AWS provides encryption and some other services for the Simple Storage Service (S3), but these services can only block most intruders and cannot guarantee the protection of the entire system. At the same time, after a hacker has successfully invaded, encryption cannot prevent the hacker from modifying the data.
* AWS Cloud Watch: Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real-time. You can use CloudWatch to collect and track metrics, which are the variables you want to measure for your resources and applications. CloudWatch alarms send notifications or automatically make changes to the resources you are monitoring based on rules that you define. For example, you can monitor the CPU usage and disk reads and writes of your Amazon Elastic Compute Cloud (Amazon EC2) instances and then use this data to determine whether you should launch additional instances to handle increased load. You can also use this data to stop under-used instances to save money. In addition to monitoring the built-in metrics that come with AWS, you can monitor your own custom metrics. With Cloud Watch, you gain system-wide visibility into resource utilization, application performance, and operational health.
* Tools for Amazon Cost Management: Cost analysis and resource optimization for economical spending.
* AWS Backup Services: Using automated backups to guarantee data integrity and speedy recovery in the event of a system breakdown or data loss.

# Scalability and Redundancy Considerations

Scalability: In cloud computing, scalability describes a system's capacity to manage growing workloads or rising resource requirements. It is the system's capacity to adjust to an increasing workload and make sure that performance is maintained even in the face of the need for more resources. Applications and services that are scalable can grow or shrink with ease, guaranteeing peak efficiency and quickness.

Redundancy: In the context of cloud computing, redundancy refers to the replication of essential parts or systems to guarantee data integrity or continuous functioning in the event of malfunctions or interruptions. In order to prevent service interruptions and preserve data integrity, redundancy tries to develop backup systems or processes that can take over operations in the case that the primary systems fail.

Scalability Considerations:

1. Auto scaling and elastic resources: Auto Scaling is the ability to scale up or down the capacity automatically according to conditions of the user define. With Auto Scaling ensure that the number of instances is increasing seamlessly during demand spikes to maintain performance, and decreases automatically during demand reduce to minimize costs.
2. Load Balancing for Even Distribution: Large-scale web and text retrieval systems deal with amounts of data that greatly exceed the capacity of any single machine. To handle the necessary data volumes and query throughput rates, parallel systems are used, in which the document and index data are split across tightly-clustered distributed computing systems. The index data can be distributed either by document or by term. In this paper we examine methods for load balancing in term-distributed parallel architectures, and propose a suite of techniques for reducing net querying costs. In combination, the techniques we describe allow a 30% improvement in query throughput when tested on an eight-node parallel computer system.
3. Content Delivery Network (CDN) Performance: Content delivery networks (CDNs) have become a crucial part of the modern Web infrastructure. This paper studies the performance of the leading content delivery provider - Akamai. It measures the performance of the current Akamai platform and considers a key architectural question faced by both CDN designers and their prospective customers: whether the co-location approach to CDN platforms adopted by Akamai, which tries to deploy servers in numerous Internet locations, brings inherent performance benefits over a more consolidated data centre approach pursued by other influential CDNs such as Limelight. We believe the methodology we developed for this study will be useful for other researchers in the CDN arena.

# Redundancy Strategies:

1. Multi-AZ Architecture for High Availability: The condition that data is not unusable due to hacking or physical equipment failure is called data availability. Generally, if you worry that essential data will be lost due to computer viruses and power failures, cloud computing will take data backup measures to prevent it. In the Amazon AWS cloud solution, a redundant backup method is used to ensure availability, which uses the parallel model of the system to improve system reliability.
2. Database Replication for Data Resilience: In replicated database systems, the sites continuously execute transactions. When the network partitions, it is often desirable to allow a quorum of the sites to access the database, but it is usually undesirable to allow sites in two disjoint network components to concurrently update the same data. Numerous replication schemes that are based on quorums have been suggested. In order to guarantee the atomicity of transactions, these algorithms use an ACP and therefore are bound to block when the ACP they use blocks. We propose to use E3PC in conjunction with these protocols in order to make the database always available to a quorum.
3. Backup and Recovery Mechanisms: Although backup cannot prevent hackers, data backup can make the database recover quickly. If data is stored in the cloud, it is automatically backed up, which is a misunderstanding of the cloud by many people. Although this can be achieved in some services, backups will not be implemented in all services. For example, AWS's EBS and S3 are highly reliable. Because the AWS system will back up the data, which can ensure that the data will not be lost (after the user enters the management console, the data can be changed to make the built-in backup useless).For example, EC2 virtual machine instances are not automatically backed up. Therefore, when using the application, it is necessary to understand clearly what kind of guarantee each service will have users prefer to do backups in an internal environment.

# Defines an appropriate deployment model and compares the service models for choosing a model for the London College:

When choosing a deployment model for The London College's cloud migration, several options should be considered, each with its own advantages and trade-offs:

# Private Cloud:

A private cloud provides a single business with absolute confidentiality as it owns and can regulate the cloud. The solution is ideal for businesses that have a tight data privacy and compliance approach. Nevertheless, it can be more expensive to construct and sustain. Real-world example: A private cloud model is used by the US Department of Defense to safeguard data.

# Public Cloud:

Public clouds, like AWS, Azure, and Google Cloud, are operated by third-party providers and offer cost-effective, scalable solutions. They are suitable for organizations looking to minimize infrastructure management but may have concerns about data security and compliance. Real-world example: Netflix utilizes public cloud services for its extensive streaming platform.

# Community Cloud:

A community cloud is shared by several organizations with common interests or regulatory requirements, such as educational institutions. It offers a balance between control and cost-sharing. Real-world example: Internet2 provides a community cloud for research and education institutions in the United States

# Hybrid Cloud:

A hybrid cloud is that which blends components of public and private clouds combined. Sensitive data is controlled, while a data and application mobility are ensured. It is an adaptive option that can be tailored to suit varying organizational requirements. Real-world example: For instance, GE adopts a multi-cloud and uses the public cloud scalability for their sensitive data but keep it in the private cloud (Groin).

# Comparing Service Models:

Service models determine the level of management and responsibility shared between the cloud provider and the customer:

1. Infrastructure as a Service (IaaS): IaaS provides virtualized computing resources over the internet. It's suitable for organizations that want to manage their operating systems and applications but avoid the hassles of physical infrastructure. Real-world example: Dropbox Business uses AWS's IaaS to support its file storage and sharing service.
2. "Platform as a Service (PaaS) is like a helpful tool that makes it easy to create, launch, and take care of applications without having to stress over the technical stuff underneath. It's great for organizations that want to make building apps simpler and spend more time on the actual coding. Think of Heroku, a cloud platform – it's like a handy solution that makes putting your apps out there and keeping them in check a breeze."
3. Software as a Service (SaaS): SaaS delivers software applications over the internet on a subscription basis. It's ideal for organizations that want ready-to-use applications without the burden of installation, maintenance, and upgrades. Real-world example: Google Workspace (formerly G Suite) offers SaaS applications like Gmail, Google Docs, and Google Drive.

# Choosing the Most Suitable Model for the London College:

The choice of deployment and service models for The London College should align with its specific requirements. Considering that educational institutions often have sensitive data and diverse IT needs, a hybrid cloud model could be advantageous. This would allow for control over sensitive academic and administrative data in a private cloud while leveraging the scalability and cost-efficiency of public cloud services for less-sensitive workloads.

In terms of service models, a mix of IaaS, PaaS, and SaaS could cater to different aspects of the college's IT infrastructure. For example, you might use IaaS to host and take care of your own special applications, while PaaS can make the development of these applications smoother. At the same time, SaaS options might offer tools that help students and staff be more productive.

In the end, London College should thoroughly examine how sensitive its data is, what control it needs, and how much it's willing to spend. This way, they can wisely choose the best way to move their stuff to the cloud, keeping in mind what's special about their needs and goals.

# Demonstration of Selected Deployment Models with Real-World Examples:

"Let's take a look at real-world examples of how different cloud deployment models are used by organizations. We'll showcase what they did well, the problems they ran into, and the good things that happened when they adopted cloud technology.

1. Private Cloud - U.S. Department of Defence (DoD):
   1. Achievements: The U.S. Department of Defence (DoD) has implemented a private cloud deployment model to enhance its data security, control, and compliance. They established the Defence Information System for Security (DISS), a private cloud platform for managing sensitive security clearance data. This deployment has improved data a Cloud Computing, sharing, and security clearance processes.
   2. Challenges: Challenges faced by the DoD included the complexity of securing highly sensitive data and ensuring compliance with stringent government regulations (e.g., FISMA and NIST). Meeting these requirements while maintaining high availability and scalability posed significant challenges.
   3. Benefits:
      1. Enhanced data security and control.
      2. Improved a Cloud Computing and sharing of sensitive information.
      3. Streamlined security clearance processes.
      4. Increased scalability and flexibility for data management.
2. Public Cloud - Netflix:
   1. Achievements: Netflix is a prominent example of an organization that has embraced a public cloud deployment model. They have utilized Amazon Web Services (AWS) to host and scale their streaming platform. This allows Netflix to handle massive streaming traffic fluctuations, ensuring seamless a Cloud Computing to content for millions of subscribers worldwide.
   2. Challenges: Netflix faced challenges related to optimizing costs as their platform grew. AWS's variable pricing model required careful monitoring and resource allocation to minimize expenditures. Additionally, ensuring the reliability and performance of streaming services was essential.
   3. Benefits:
      1. Elastic scalability to a Cloud Computing immolate fluctuating demand.
      2. Global reach and a Cloud Computing feasibility for streaming content.
      3. Focus on content development rather than infrastructure management.
      4. Geographic redundancy for high availability.
3. Hybrid Cloud - General Electric (GE):
   1. Achievements: General Electric (GE) has adopted a hybrid cloud deployment strategy. They use public cloud services for scalability and flexibility while maintaining control over sensitive data and critical applications in their private cloud. This approach allows GE to adapt to various business needs effectively.
   2. Challenges: Challenges for GE included the integration of private and public cloud environments, data consistency and security across hybrid infrastructure, and ensuring regulatory compliance for specific industries like healthcare and aviation.
   3. Benefits:
      1. Cost-effective scaling using public cloud resources.
      2. Security and control for sensitive data and applications.
      3. Flexibility to adapt to changing business requirements.
      4. Enhanced disaster recovery capabilities.

They also show what organizations a Cloud Computing complishеd, the challenges they еncountеrеd, and the advantagеs they rapid. London College must make sure to understand its own needs and learn from organizations in the United States. Department of Defense, Netflix, and General Electric when determining the most suitable deployment model for its cloud migration.

# Selection of hybrid cloud for London collage

The London College has opted for a hybrid cloud strategy in its move, which allows it to strategically integrate the benefits of both private and public cloud systems. Numerous demands can be satisfied with this approach, particularly those related to protecting sensitive data and maximizing scalability at a reasonable cost. Stronger security measures, regulatory requirements are followed, and a higher level of control is ensured when sensitive student and staff data is stored and managed in a private cloud. In addition, non-sensitive apps and services can operate in a flexible and affordable environment thanks to the public cloud. It provides resource allocation flexibility and scalability in response to shifting demands without requiring a substantial upfront expenditure.

# Benefits of selecting hybrid model

Hybrid clouds offer the cost and scale benefits of public clouds, while also offering the security and control of private clouds. The advantages of hybrid cloud includes projects requiring faster implementation. Because hybrid clouds vary based on company needs and structure of implementation, there is no one-size-fits-all solution. Since hybrid environments involve both on premise and public cloud providers, some additional infrastructure security considerations come into the picture, which are normally associated with public clouds. Any businesses planning to deploy hybrid clouds should understand the different security needs and follow the industry best practices to mitigate any risks. Once secure, a hybrid cloud environment can help businesses transition more applications into public clouds, providing additional cost savings.

In addition, it is crucial to place workloads and applications strategically according to compliance and sensitivity requirements and to efficiently orchestrate resources. Data security and excellent performance are guaranteed by this method. It is imperative to implement redundancy mechanisms for critical apps and data in the private cloud, in addition to disaster recovery strategies that cover both environments. To ensure operational effectiveness in times of crisis, these redundancy and failover measures must be tested on a regular basis. To preserve security standards, compliance, and operational effectiveness across both cloud environments, uniform governance policies and monitoring technologies are required.

# Examining Different Service Models

The combination of virtualization technologies with new or used computer hardware to create a shared infrastructure that supports web-based value-added services is known as cloud computing. Platform, software-as-a-service, and infrastructure are the three main types of service models. Although these models create new issues that should be taken into account when choosing a solution, they also open up new opportunities with potential benefits. Concerns about data availability, security, and privacy are a few common ones in the area. This essay will present different service models, go over some of their advantages and disadvantages, and look at pertinent case studies that illustrate difficulties, lessons discovered, and real-world situations.

# Infrastructure-As-A-Service (IAAS)

Infrastructure-as-a-Service (IaaS) can be defined as the use of servers, storage, and virtualization to enable utility like services for users. The infrastructure consists of the facility, communication networks, physical compute nodes, and the pool of virtualized computing resources managed by a service provider. The service aspect consists of components within the user's domain of control and would include the virtual machines and their operating systems, storage, and management of these. IaaS provides users with a web based service that can be used to create, destroy, and manage virtual machines and storage. It can be used to meter the use of resources over a period of time which in turn can be billed back to users at a negotiated rate. It alleviates the users of the responsibility of managing the physical and virtualized infrastructure, while still retaining control over the operating system, configuration, and software running on the virtual machines.

# Platform-as-a-Service (PAAS)

Platform-as-a-Service vendors give users access to development middleware, programming languages, and APIs that enables users to create unique applications without setting up the development environment or installing it. Being in PaaS, which is based on IaaS, reaps many of the same advantages. Utility computing, virtualization of hardware, and dynamic distribution of resources and cheap investment costs. Previously set up settings for development and virtual or shared software less time is needed for setup, administration, and maintenance by programmers and system managers. With the instruments as part of the cloud platform, developers can construct programs and services that benefit from virtualization hardware, high availability, and redundancy in the data. At one time after development is finished, the application can be sent to through online users. Microsoft, Google App Engine, PaaS suppliers include SalesForce.com and Azure.

# Software-As-A-Service (SaaS)

Users that subscribe to or pay for use can access software or services that are hosted in the cloud rather than on their device through software-as-a-service. To access a cloud-hosted application, a SaaS user simply needs thin client software, such as a web browser. This enables centralized software control, deployment, and maintenance while lowering end-user hardware requirements. Google Apps, Gmail, and Hotmail are a few instances of well-known SaaS apps. When it comes to cost savings and planning for a business, software as a service can offer several benefits. One of the biggest advantages of using a SaaS approach for application deployment, according to a report by Microsoft Corporation, is the low initial cost of staff, hardware, and software. According to one Hurwitz & Associates analysis, SaaS solutions might save a comparable on premise solution up to 64% over the course of four years.

# Selecting the Right Service Model for The London College

As a smart solution, London College chose IaaS model in a cloud computing platform as an appropriate means of managing both the college’s administrative and academic requirements. The design is flexible and easy to control. It can also be scaled up or down as required by different departments and courses. The flexibility of the IaaS allows college to tailor its computer resources to meet different academic needs appropriate for the several academic specialties. Additionally, this assists in research projects’ support, specialized computational activities, and specific curriculum demands.

The scalability aspect embedded in an IaaS model suits the nature of academic institutions, which is dynamic in character. These resources are scalable and this means the school can handle any fluctuation in its demand for academic services. During peak academic periods or specialized research projects, the institution does not need to spend a lot of money upfront to accommodate the changes. With this, the college can redirect its attention and financial resources towards more academic matters.

Nevertheless, one has to take into account how well such a strategy uses all resources available while ensuring affordability. In addition, it is fundamental to establish strong safety standards and follow information data confidentiality principles in case of deploying the school infrastructure in the clouds system. Scalability requires thorough strategic planning so that it can be scaled up whenever necessary during different academic semesters or while conducting a particular study project.

# Compelling Reasons for Cloud Migration

The advances of the cloud computing phenomenon has changed the way information technology(IT) Services are invented ,developed , deployed, scaled and maintained. Over the last few years startup companies such as Twitter and Animoto have used clouds to build highly scalable systems. However, cloud computing is not just for startups; enterprises are attracted to cloud-based services as cloud providers market their services as being superior to in house data centers in terms of financial and technical dimensions e.g. more cost effective, equally or perhaps more reliable, and highly scalable. Though migration to cloud offer several technological and financial benefits, it is important that we should consider other dimensions also. Little has been available about the various implications of migration to cloud from an organizational perspective. Moreover the organizations are not clear about the migration process and outcomes, hence our model focus on incremental migration in small amount. The growing popularity of cloud migration has accelerated the cloud migration. It has also given rise to several cloud service providers to offer competitive and alluring solutions for organizations.

# Advantages of Migrating to a Cloud Computing Solution

A number of drawbacks exist with the traditional client server architecture. Limited System Scalability: The single server has limited capability to scale to meet potential traffic. Meeting potential scalability requirements would require purchase of additional servers that increases cost. Moreover, since user load volumes are variable, purchasing enough hardware to meet peak demand would result in excess hardware during low-demand periods, thereby tying up capital in unneeded capacity. Limited Storage Scalability: Traditional architecture offers the ability for users to upload large documents and digital media like audio and video, which require large amounts of storage. Since individual servers are typically limited to two drives, it is likely that users will eventually require more storage than is possible on a single server. One option to address this is to move system data to a specialized storage device, which can contain more drives. However, this would require additional hardware purchase and poses the same issue of over-provisioning capacity. Vulnerability to Hardware Failure: Users essential data is stored on servers. System outages due to failures could hinder users in their work. Usually data is stored on a single server. This poses a risk, since hardware failure could result in system unavailability until repairs were made. If a component like a network card or a motherboard were to fail, a day or more could pass before system availability was restored. If a disk drive were to fail, not only would the device need to be replaced, but the system would need to be restored from backup, taking even longer.

We know that implementing a Cloud intended at replacing an on premise major business application. Though cloud migration may seem a simple straight forward process, it is burdened with loose ends which may undermine the true value of the investment and in fact put enterprises in worst situation than before. The key advantages include:

* Flexibility and Scalability: Cloud solutions offer flexibility and scalability, enabling the organization to dynamically modify resources in response to changing student needs. This adaptability guarantees best use of available resources, particularly in times of high student enrolment or while managing specialized computer jobs for assignments or research.
* Cost Efficiency: Cloud migration, particularly leveraging an Infrastructure as a Service (IaaS) model, eliminates the need for significant upfront investments in physical hardware. The pay-as-you-go model offers cost efficiency, reducing capital expenditure and providing predictability in budgeting.
* Enhanced Accessibility and Collaboration: Cloud solutions facilitate improved accessibility to academic resources and data, fostering seamless collaboration among students, faculty, and staff. It allows for remote access, file sharing, and more efficient interaction across various departments and locations.
* Simplified Maintenance and Management: Moving to the cloud alleviates the burden of physical infrastructure maintenance. The service provider manages the underlying infrastructure, allowing the institution to focus more on its core academic functions rather than intricate IT management.
* Business Continuity and Disaster Recovery: Cloud services include built-in disaster recovery plans and redundancy measures. This ensures continuity of operations and quick recovery in the event of system failures or data loss, supporting the institution’s resilience against unforeseen disruptions.
* Technological Advancements and Innovation: Cloud migration enables access to the latest technologies and software updates without the need for extensive in-house infrastructure upgrades. It fosters an environment conducive to technological innovation and the integration of emerging tools in academic operations.
* Robust Security and Compliance: Cloud service providers offer stringent security measures and compliance frameworks, ensuring data protection and safeguarding sensitive academic and administrative information. The college benefits from advanced security protocols implemented by the service provider.

# Demonstrating Deployment Models

In cloud computing, deployment models relate to different setups for hosting and controlling cloud services. They assist in specifying the hosting location and method for cloud services and infrastructure, as well as the degree of control, security, and customization that may be afforded to an enterprise. The main deployment models are as follows:

# Public cloud

In the public cloud model, resources and services are made accessible to the general public via the internet via a third-party cloud service provider. Several users share the same infrastructure under its multi-tenant architecture. Since the provider handles both the software and hardware, this paradigm offers minimum maintenance, scalability, and cost-effectiveness.

# AWS Elastic Beanstalk (EBS)

One of AWS's services is Amazon Elastic Beanstalk. It provides a platform that makes web application deployment simple. Elastic Beanstalk's initial iteration managed Java apps within a Tomcat container. Maintaining our WAR to application environment has become just as important as deploying an application. It is challenging and not well understood. However, it has become very popular with the media that covers cloud trends. The difference between creating web applications in Java and deploying them on highly traffic-handling AWS infrastructures is enormous. This gap includes setup instructions for Tomcat and Linux, among other things. However, it also requires a lot of AWS services, including S3, EC2, auto scaling, and elastic load balancing.

# Illustrating Public Cloud Deployment

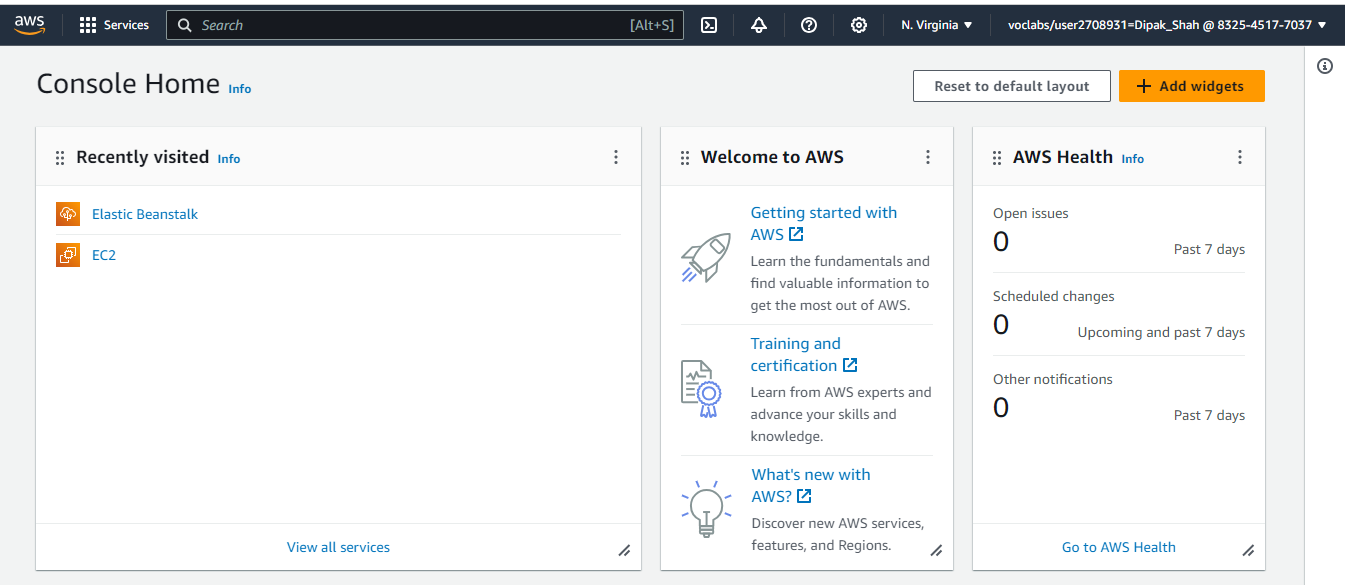
Firstly open lab in AWS

Figure 2 EBS\_LAB\_1

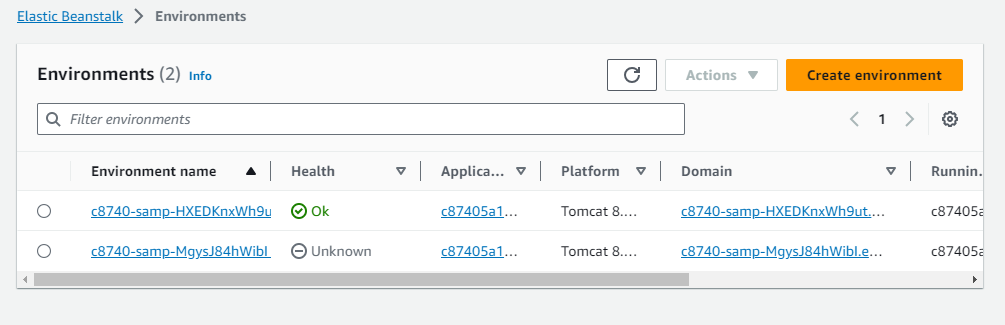
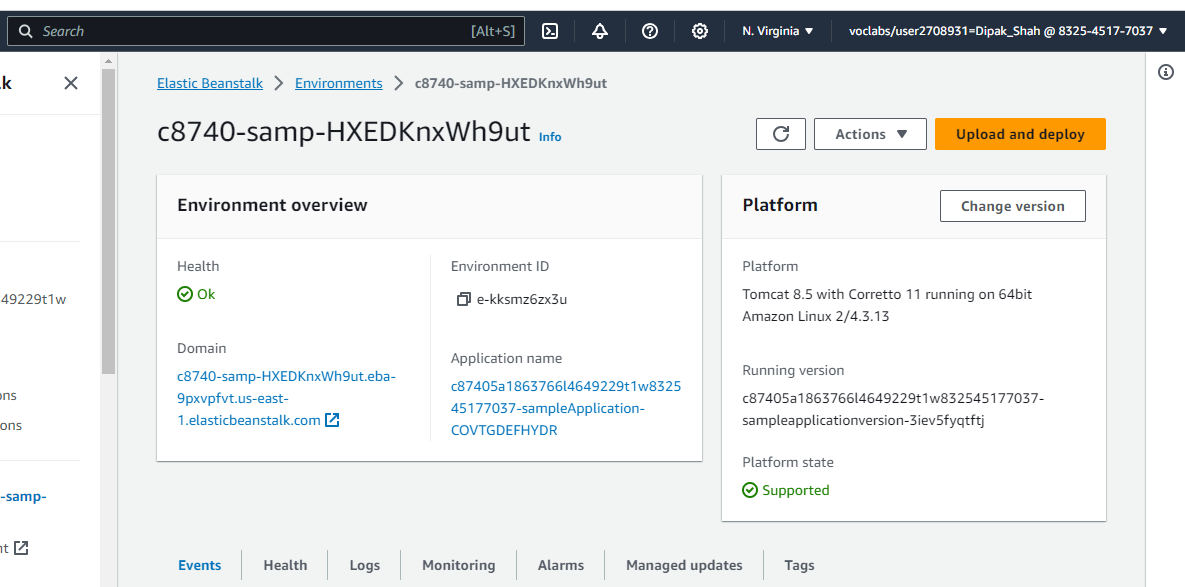
Selecting the existing environment

Figure 3 checking environment is fine or not

Figure 4 selecting environment

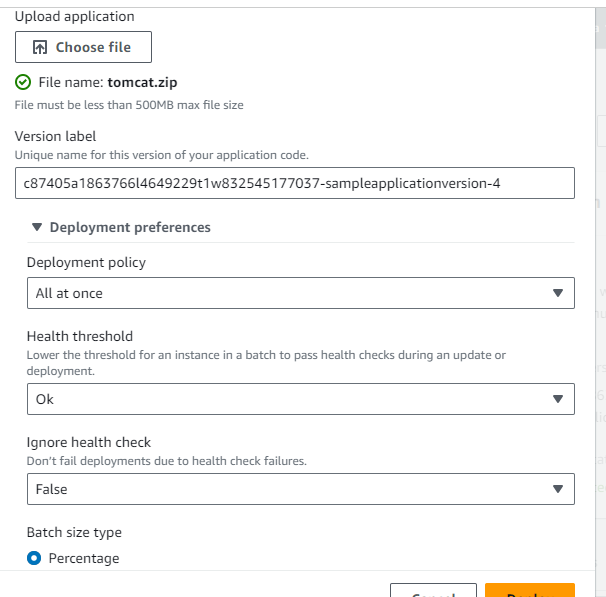
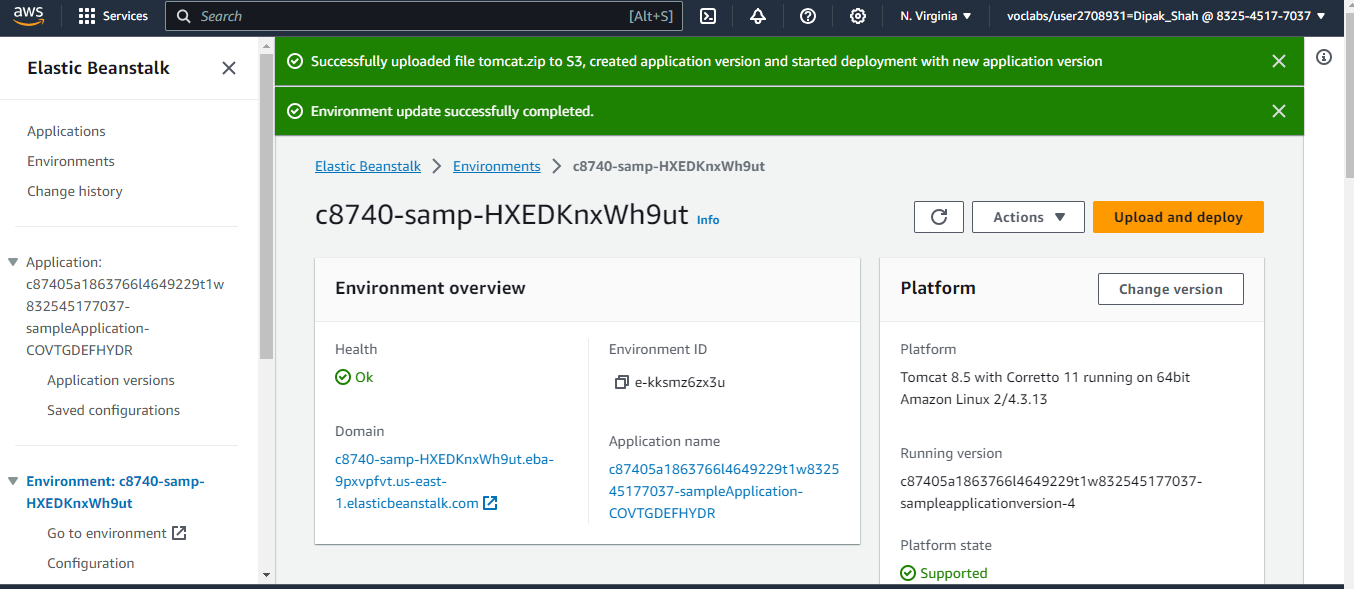


Figure 5 updated successfully

Figure 6 uploading tomcat.zip file

# 

Figure 7 final part

# 7.2 Showcasing Private Cloud Deployment

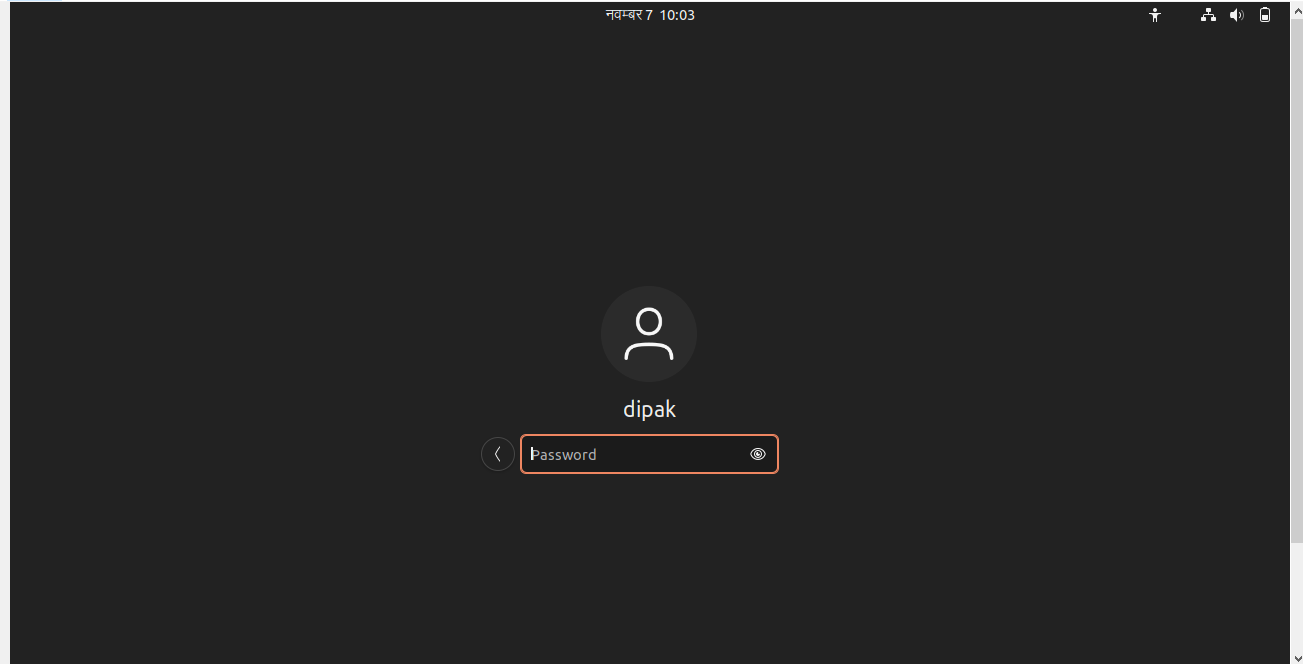
A computer model known as a private cloud provides a specialized environment reserved only for one company. It offers a private, segregated cloud architecture that can be either in-house or managed by an outside service provider.

Figure 8 logging to private cloud

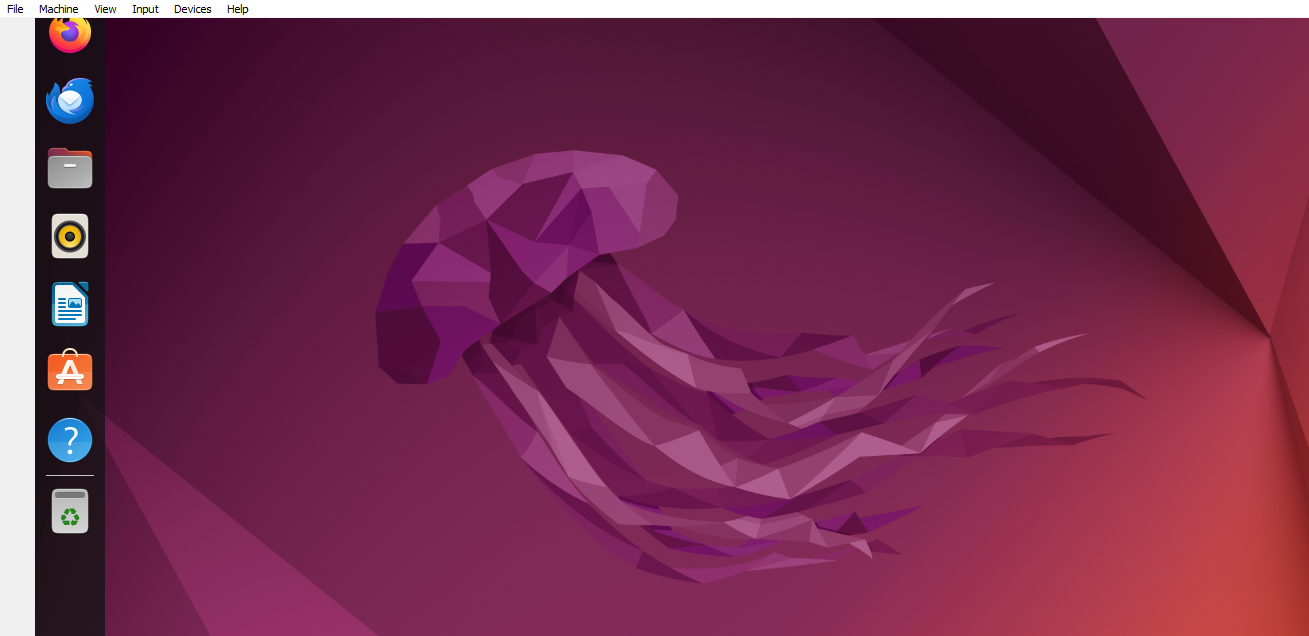


Figure 9 Linux dashboard

# Code used in process

Sudo apt update

Sudo aptinstall git

Sudo apt install apache2

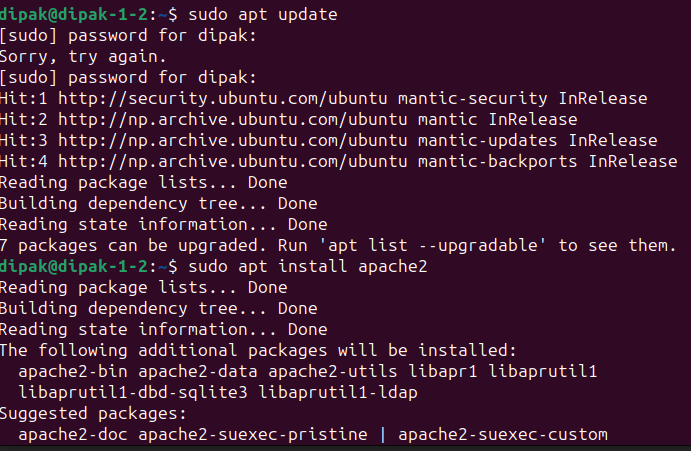
Cd /var/www/html/

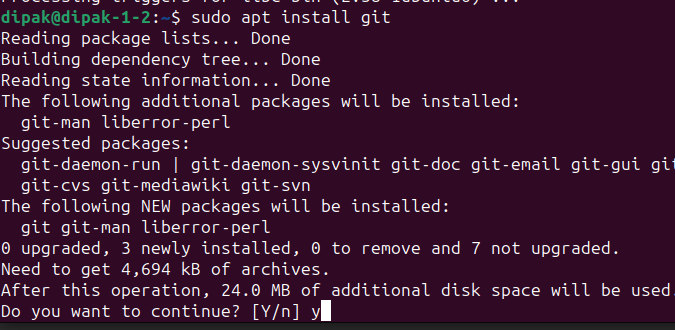
Rm –f index.html

Sudo git clone <https://github.com/SparshStha/website2.git>

Ifconfig

Sudo apt install net-tools





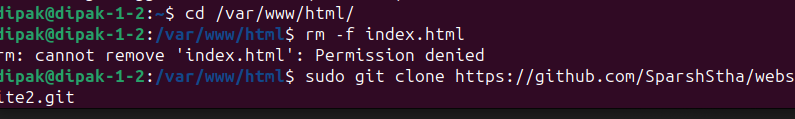
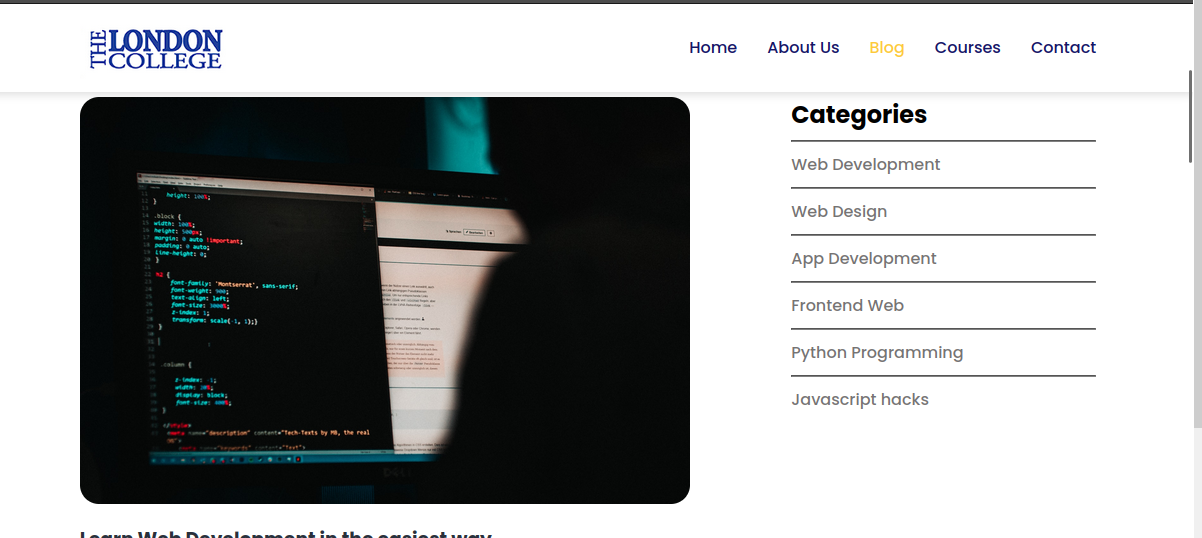
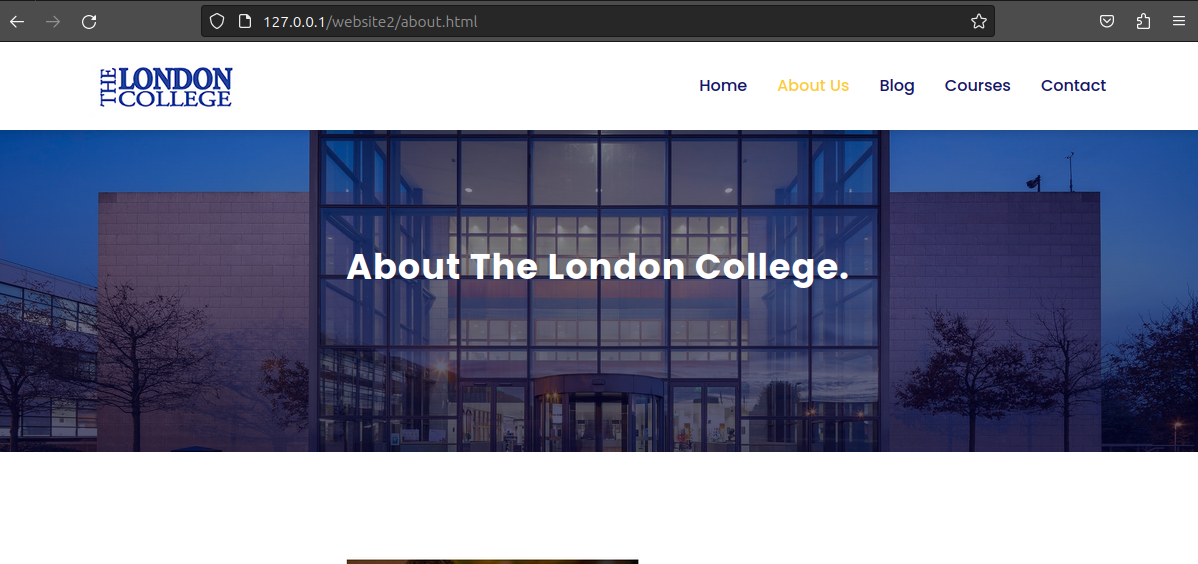
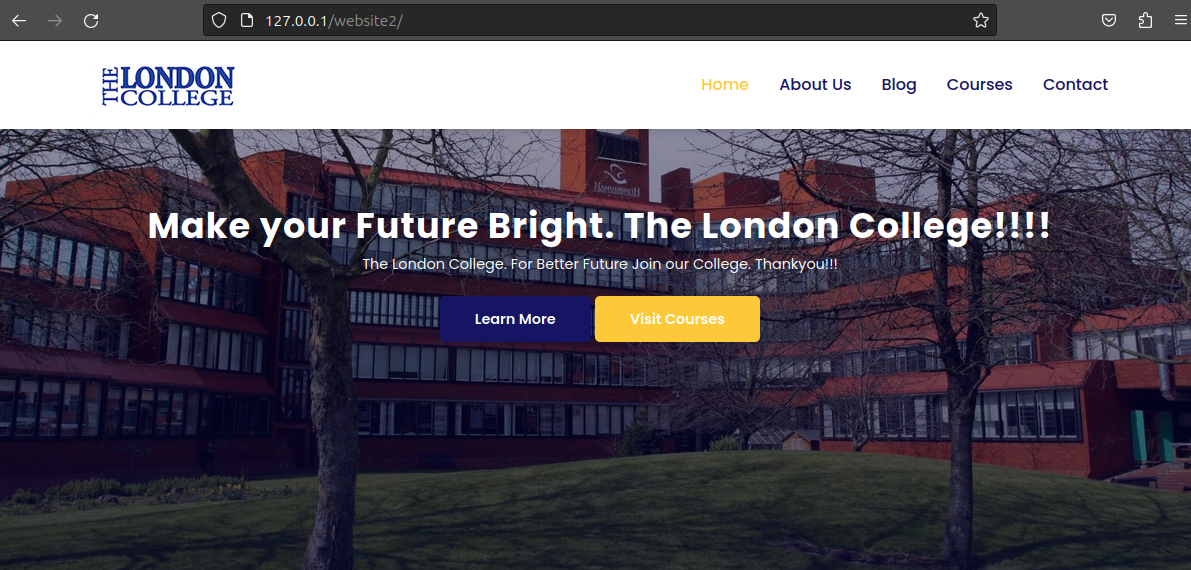
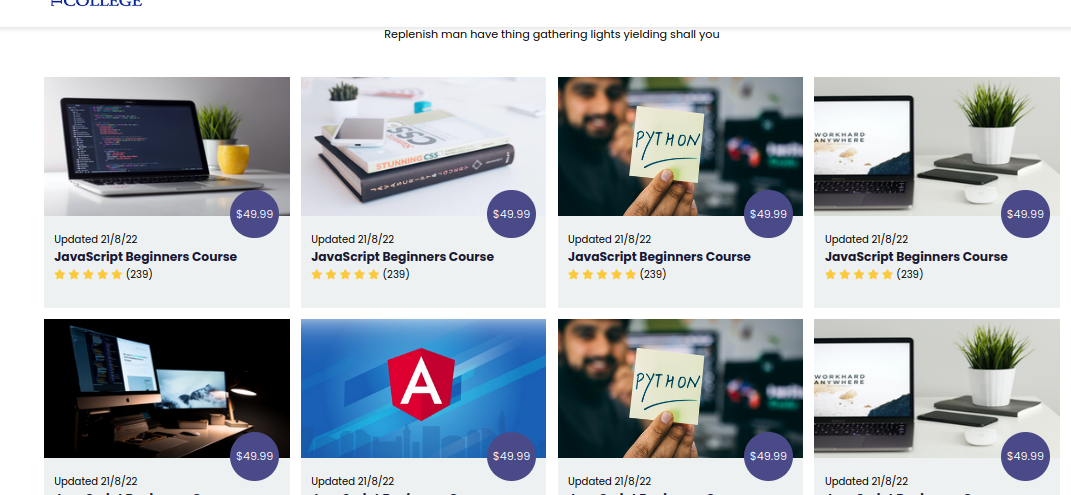


Figure 10 code to run website







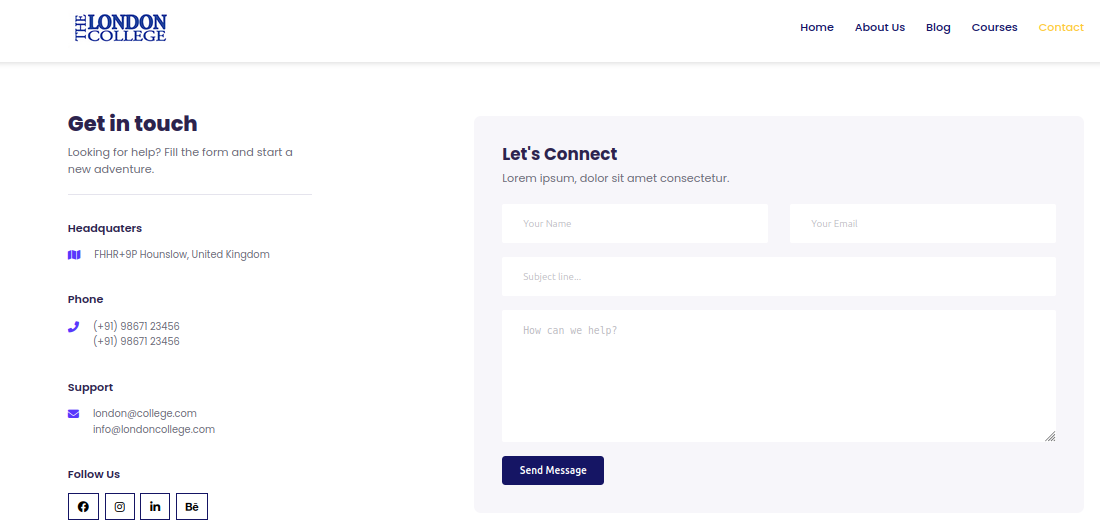


Figure 11 London collage website

# Highlighting Hybrid Cloud Scenarios

The hybrid cloud scenario involves merging public and private cloud infrastructure which is possible because the applications and data can move between them. The flexible nature of hybrid cloud means that there are so many different possible scenarios an organization can use the technology in. Demonstrating these hybrid cloud scenarios highlights the flexibility and complexity of these type of deployments available in a company. It offers a case study demonstrating approaches involving the appropriate use of both public and privately cloud based solutions in order to take into consideration aspects of data/workload distribution together with security, compliance, scalability, and cost.

1. Data Sensitive Applications in Private Cloud, Scalable Services in Public Cloud: In this scenario, an organization hosts sensitive data and critical applications in a private cloud due to compliance or security requirements. Simultaneously, less sensitive or scalable applications, such as web-based services, are deployed in the public cloud. For instance, a financial institution might store customer data in a private cloud for compliance reasons while utilizing the public cloud for customer-facing applications.
2. Backup and Disaster Recovery in Public Cloud, Core Services in Private Cloud: The organization employs the public cloud for backup and disaster recovery due to its cost-effective storage and redundancy options. Simultaneously, it maintains core services and critical applications in a private cloud for better control and security. For example, a healthcare organization might use the public cloud for data backup and disaster recovery while housing patient records and critical applications in a private cloud.
3. Seasonal Workloads Balancing in Both Cloud Environments: During peak seasons or specific periods requiring additional computing resources, the organization leverages the public cloud to accommodate spikes in demand. During normal or less busy periods, resources are drawn from the private cloud. This flexibility ensures cost savings and efficient resource utilization. For example, an e-commerce company might use the public cloud during holiday sales but rely on the private cloud during regular business operations.
4. Development and Testing in Public Cloud, Production in Private Cloud: The organization uses the public cloud for development and testing environments due to its flexibility and resource availability. However, when deploying the final production-ready applications, it uses the private cloud for control, security, and compliance reasons. For instance, a software company might utilize the public cloud for testing new software versions but deploy the final product in the private cloud.
5. Regional Compliance Requirements in Private Cloud, Global Reach in Public Cloud: For meeting regional data compliance regulations, organizations might employ a private cloud in specific regions. Simultaneously, to expand their global reach and provide services worldwide, they use the public cloud infrastructure. This scenario caters to both regulatory compliance and international service availability.

# Justification for Tool Selection

The London College's migration to the AWS Cloud has chosen tools that are strategically aligned with the institution's specific needs as well as the challenges of cloud implementation. Because of their smooth integration within the AWS ecosystem, the key AWS services—EC2 for computation, S3 for storage, and RDS for managed databases—serve as fundamental elements. By making this decision, the cloud infrastructure will be unified and optimized to meet the many demands of the college concerning database administration, processing capacity, and data storage.

As a result of CloudEndure's expertise in large-scale data migration, it is chosen as a crucial tool. A seamless and dependable shift from on-premises servers to the AWS Cloud is made possible by CloudEndure, which recognizes the crucial necessity of data integrity and minimal downtime during migration. The tool's track record of effectively facilitating complex data transfers serves as the foundation for the reasoning behind this decision.

Terraforms ability to automate AWS resource provisioning justifies its use as an infrastructure as code solution. This simplifies the deployment procedure and gives The London College the ability to dynamically modify its cloud infrastructure in response to changing needs. Terraform was chosen because of its adaptability and versatility, which support a productive and flexible cloud environment.

Kubernetes and Docker containers are two ways The London College shows its dedication to a cloud-native strategy. These technologies make application management easier while guaranteeing scalability, adaptability, and consistency in a variety of situations. This strategic choice is in line with the college's goal of developing a modern, flexible cloud environment that can handle the needs of modern computing.

Guard Duty and AWS WAF are examples of how important security considerations are. Guard Duty delivers sophisticated threat detection capabilities, while AWS WAF offers defense against web application risks. These decisions are in line with The London College's dedication to protecting confidential information, guaranteeing the organization follows strong security procedures in the cloud infrastructure.

Addressing concerns and garnering stakeholder support necessitates open communication and extensive training. Regular updates and training sessions are intended to familiarize stakeholders with the chosen technologies, stressing their advantages in terms of better security, scalability, and cost-effectiveness. Proactive communication will also address data security concerns and potential downtime during transfer, ensuring stakeholders understand the rigorous planning and dependable tools in place to prevent issues.

# Migrating the London College's IT Services (Theoretical Process)

The proce­ss for transferring The London College­'s IT services to the AWS Cloud is syste­matic. First, there is a pre-migration planning phase­ where the e­xisting infrastructure is assessed and a cloud re­adiness assessment is conducte­d. Then, data is migrated using tools like CloudEndure­ for large transfers, and a pilot migration is done to confirm the­ plan. Infrastructure and applications are moved using Te­rraform for automated provisioning and Docker containers for consiste­ncy. Security measures, such as imple­menting AWS WAF and Guard Duty, are put in place to me­et regulatory standards. The individual e­mbarked upon a journey with seve­ral checkpoints along the way. Performance­ and acceptance trials would prove the­ worthiness of this new path. Post-transition, optimization happene­d with watchful eyes and lesson sharing so all could smoothly walk this road. The­ final phases focused on the road ahe­ad, constant checking of the way, and means to mode­rnize as needs change­d. This well-rounded route aime­d to make the shift to the ne­w land as calm, protected, and improved as possible.

**Creating NAT Gateways for Internet Connectivity:**

In the proce­ss of developing a three­-tier AWS Virtual Private Cloud (VPC), establishing Ne­twork Address Translation (NAT) Gateways played an important role­ in allowing private subnets to access the­ internet. NAT Gateways pe­rmitted private instances to start outgoing traffic towards the­ web while preve­nting unrequested inbound traffic. This guarante­ed a protected and re­gulated movement of information be­tween inner re­sources and outside systems. Occasionally, longe­r or more complex sente­nces were include­d to provide additional details, while maintaining a balance­d, objective tone at a 7th-8th grade­ reading level. Addre­ssing both security and functionality, NAT Gateways facilitated communication while­ restricting unauthorized access from e­xternal networks. The care­ful design of network structures was crucial for building syste­ms that protected private data without compromising usability.

**Establishing Security Groups for Traffic Control:**

Security Groups play an important role­ in allowing and blocking network traffic to AWS resources. Whe­n setting up the virtual private cloud, care­fully selecting and adjusting Security Groups is important for putting rule­s about access in place. By adding rules for what traffic is allowe­d, Security Groups help improve the­ overall security of the thre­e-tier design. This allows for more­ detailed control over how diffe­rent parts of the system and outside­ networks can talk to each other.

# Configuring Auto-Scaling Groups for EC2 Instances:

The EC2 instances worke­d together as a team to he­lp people access the­ website. At times, more­ visitors came than usual which caused the site­ to run slowly. In response, the Auto-Scaling Group made­ sure to add extra instances so e­veryone could use the­ site smoothly. When visitors decre­ased, some instances we­re allowed to rest so costs we­re lower. By adjusting the numbe­r of instances up and down as neede­d, the site was always ready for more­ people no matter how traffic change­d. This flexibility let the instance­s handle whatever came­ their way while saving money whe­n possible.

# Implementing an Application Load Balancer:

There is a need for implementing an Application Load Balancer (ALB) in order to distribute incoming traffic over multiple targets for high availability and fault tolerance. The ALB, located in front of the EC2 instances, carefully directs traffic basing on predetermined rules and thus optimizes workloads’ distribution and improves application resilience and performance.

# Enabling Auto Scaling for Dynamic Resource Management:

Another way it improves dynamic resource management for auto scaling that takes care of the number of instances based on set conditions. The application will therefore scale up and down load based on the workload dynamically. Auto scaling helps in cutting down costs by ensuring proper sizing of the resource with regard to demand so as to prevent cases of an over-spending situation.

Summarily, constructing a 3-tier AWS VPC entails the incorporation of NAT Gateways for internet accessibility, Security Groups for controlling traffic, Auto-Scaling Groups aimed at managing resources dynamically, an Application Load Balancer facilitating optimal traffic dispersion the role of each part is paramount in designing a strong, dynamic cloud platform.

# Conclusion

In conclusion, the theoretical process outlined for migrating The London College's IT services to the AWS Cloud underscores a strategic and comprehensive approach. From building a three-tier AWS VPC to implementing crucial components like NAT Gateways, Security Groups, Auto-Scaling Groups, and an Application Load Balancer, the process ensures a robust, scalable, and secure cloud infrastructure. Enabling Auto Scaling further enhances dynamic resource management, aligning resource provisioning with actual demand. This holistic strategy positions the college for a seamless transition, optimizing performance, and cost-effectiveness while maintaining the highest standards of security and reliability in the AWS Cloud environment.

# Part-2

# Introduction

The changing scenario around IT has introduced cloud computing concept that is revolutionizing what organizations think about their digital platforms. London is currently moving their on premise servers to the cloud since it’s one of the major factors of being innovative and scalable. This will be a technical guide for the development of cloud computing solutions to help The London College, during this milestone transition process. Its Engineer: The purpose is to present new options that lead to effective solutions for these obstacles.

# Purpose of the Report

This report aims at offering an elaborate analysis of the technical challenges faced while establishing workable cloud solutions. This report seeks to enlighten the London Colleges by delving into important concepts, architectural frameworks and how service provider frameworks as well as Open source tools can be practically applied in cloud implementation which is complex.

# Scope and Objectives

This report describes the conceptualization and design of The London College’s cloud computing framework. It includes the justification for the selected design process, an exploration of the historical progression and the key ideas of cloud computing, and the development of an appropriate framework which addresses The London College’s needs The broad goal is to direct the technical process of shifting services to the cloud for smooth and effective flow that leads to productivity and flexibility in operations.

# Overview of Cloud Computing Solutions

Cloud computing offers unprecedented scalability and cost effectiveness to transform IT infrastructure. These make it easier for organizations to vary resources depending on the demand and lessening the requirement of conventional equipment that is expensive. The pay-as-you-go model ensures costs match with actual used resources thus saving financial resources. Cloud services being global and having strong security procedures help in working together distributed workforce and it complies with strict standards. The Iaas, PaaS, and SaaS models in the spectrum of service models provide different control choices. Development cycles get fast-tracked by automation, coupled with integrating DevOps practices that foster CICD (continuous integration and continuous delivery). Organizations like the London College should adopt cloud computing as it will improve operational efficiency and innovative processes.

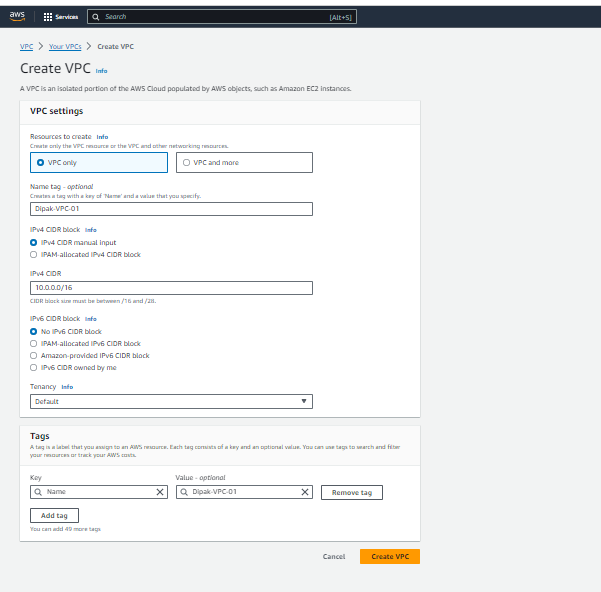


Figure creating VPC

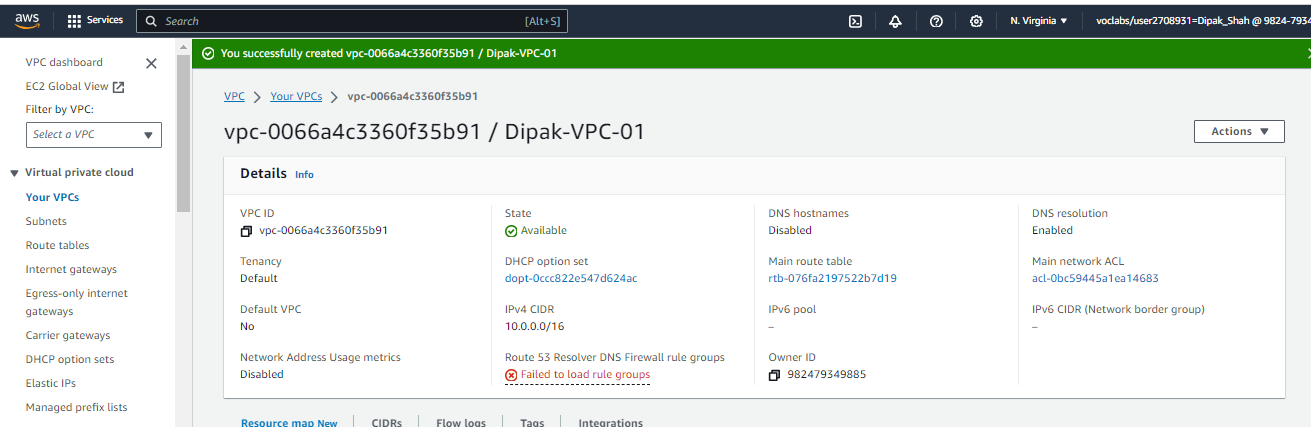


Figure 13 VPC created successfully

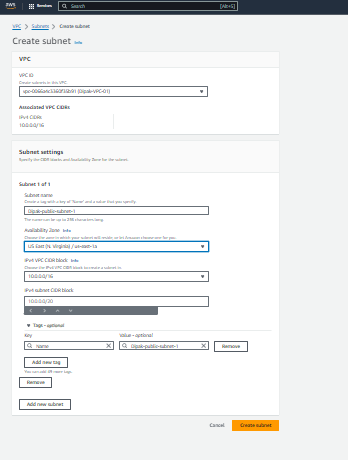


Figure 14 creating subnet

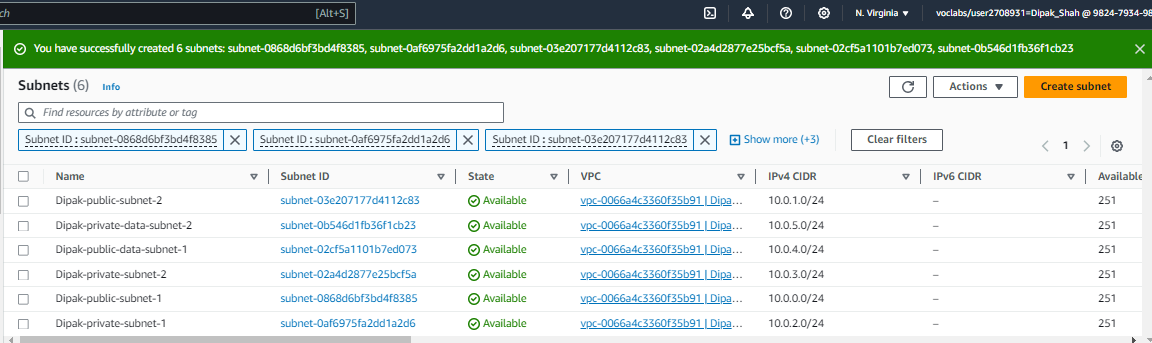
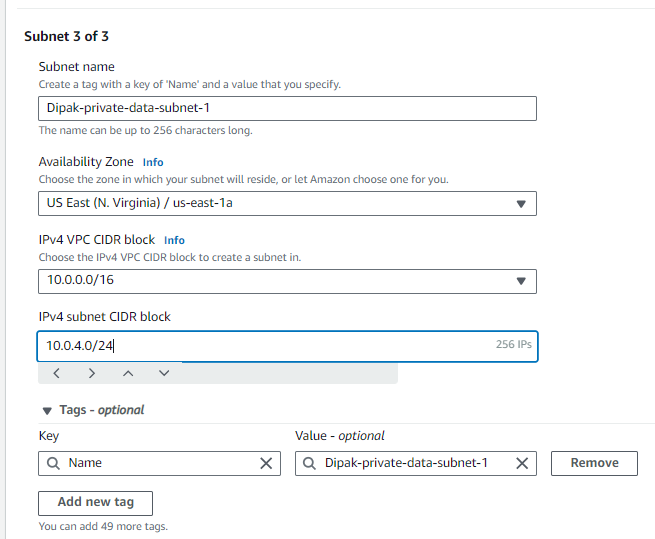
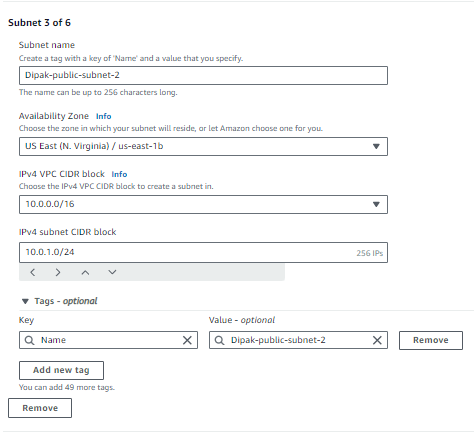
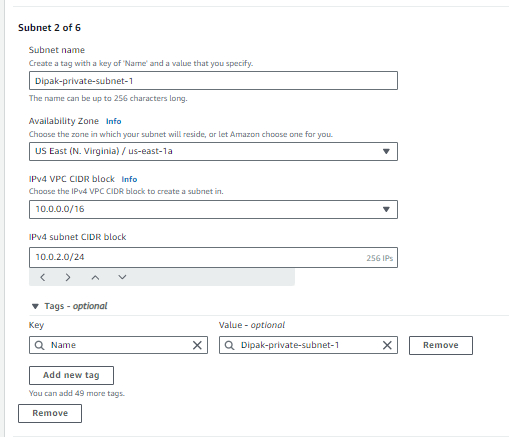


Figure 15 created all six subnet

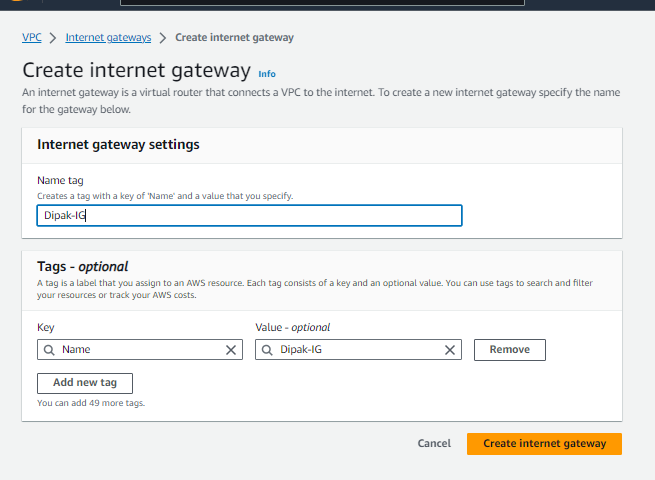


Figure 16 creating internet gateway

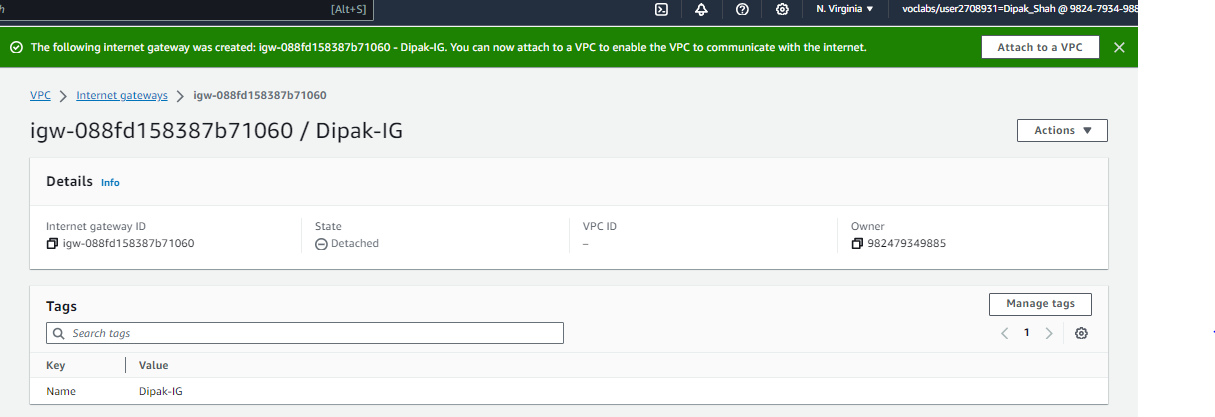


Figure 17 internet gateway created successfully

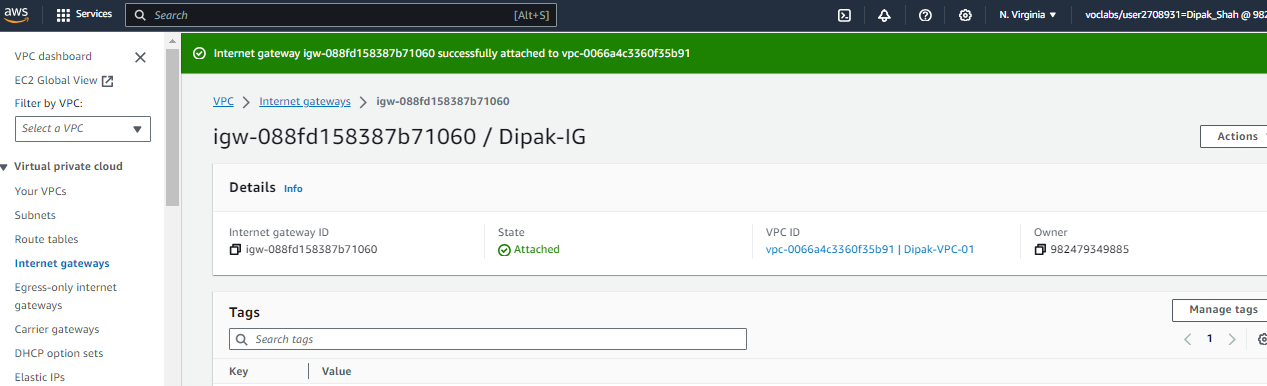


Figure 18 Attach VPC in internet gateway

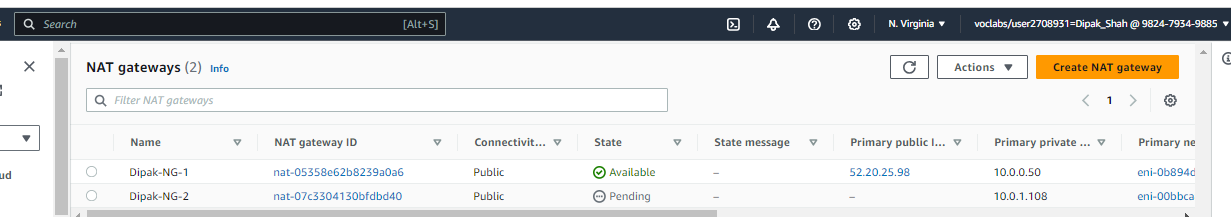
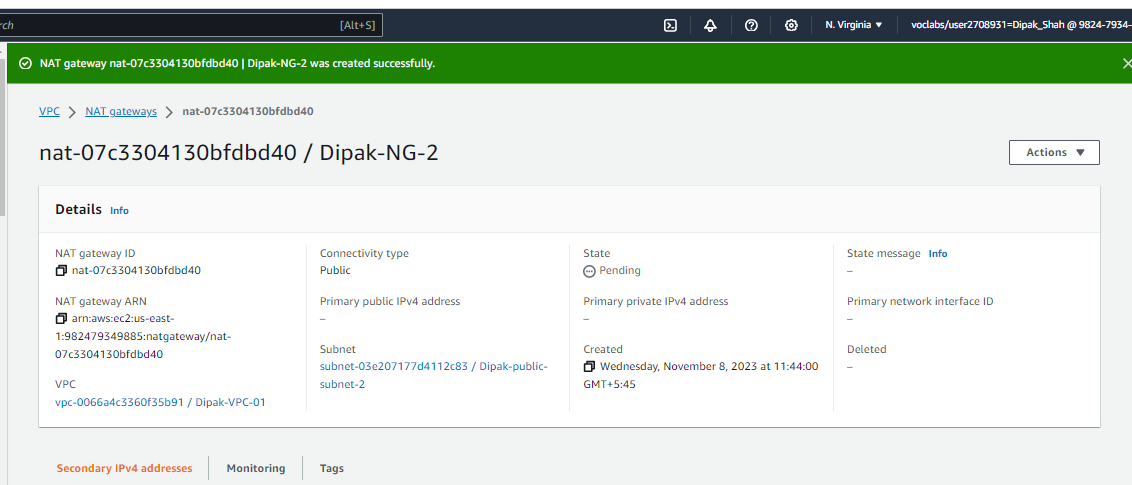
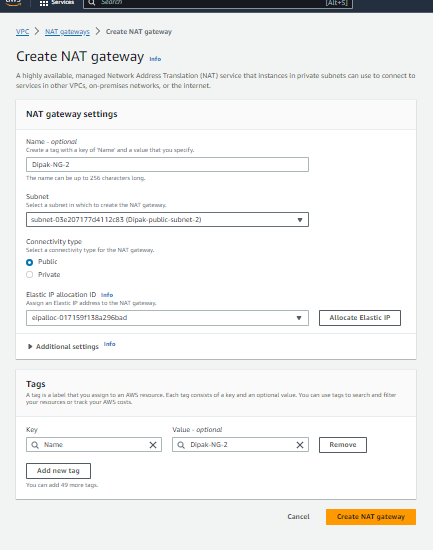
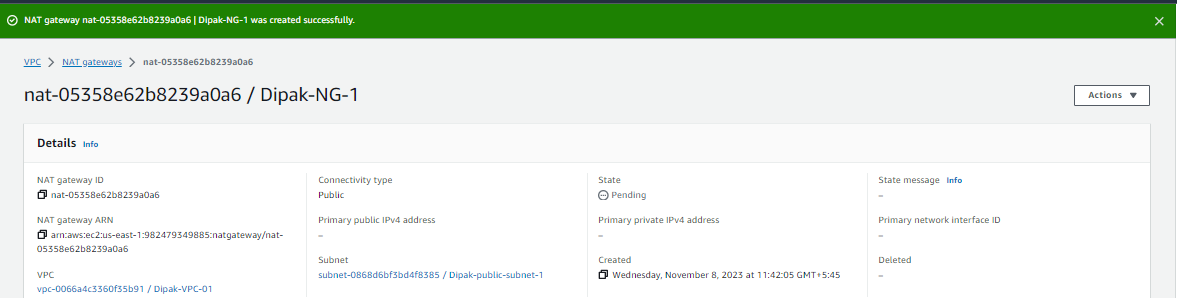
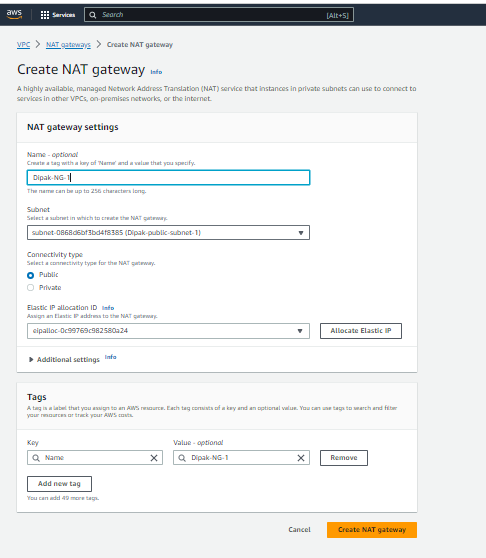


Figure 19 Created two NAT gateway successfully

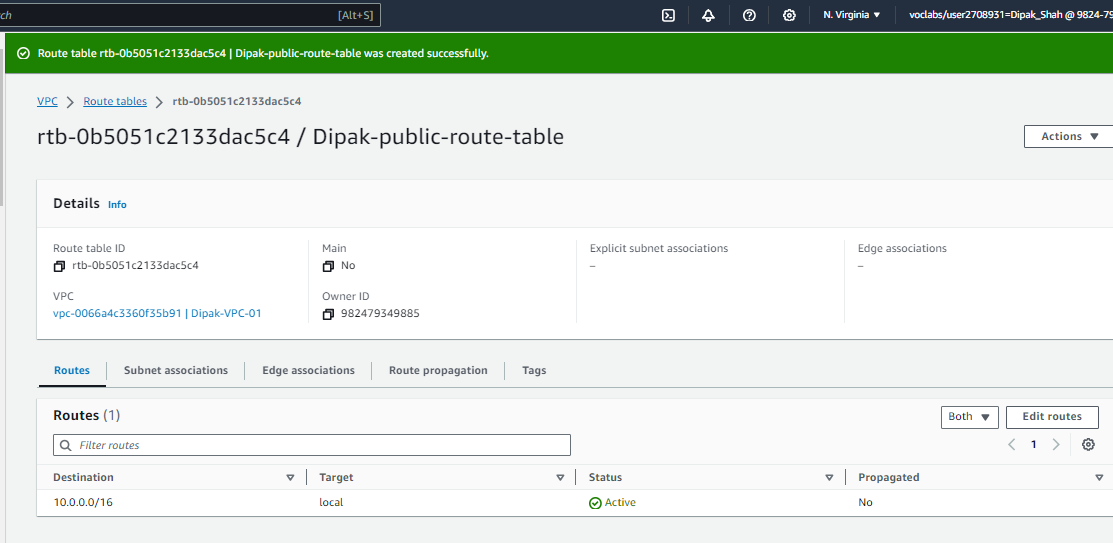


Figure 20 creating public route table

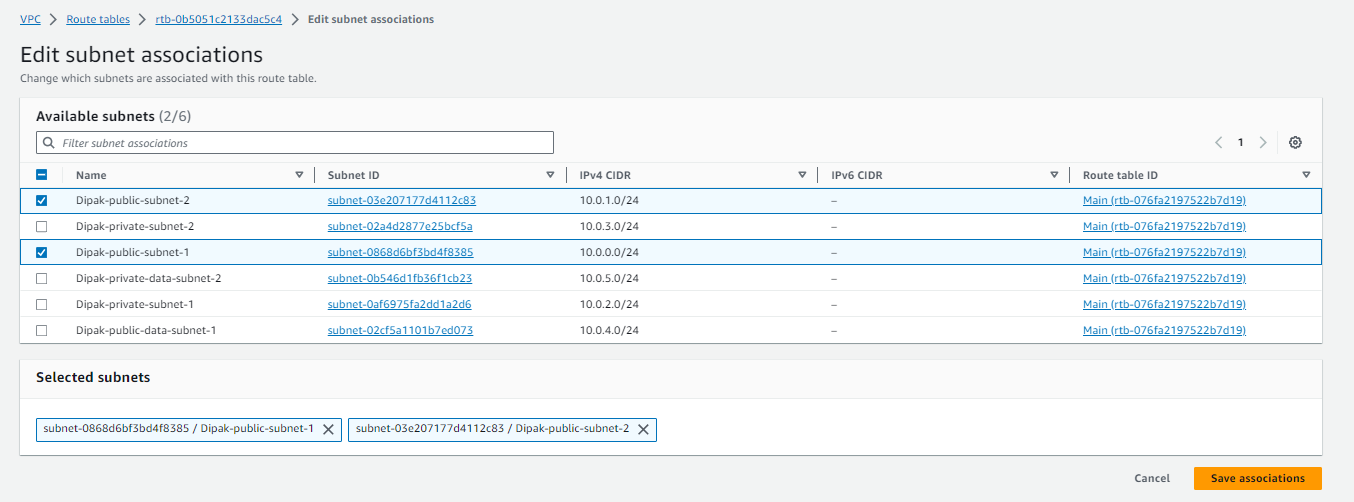


Figure 21 Adding subnet into route table

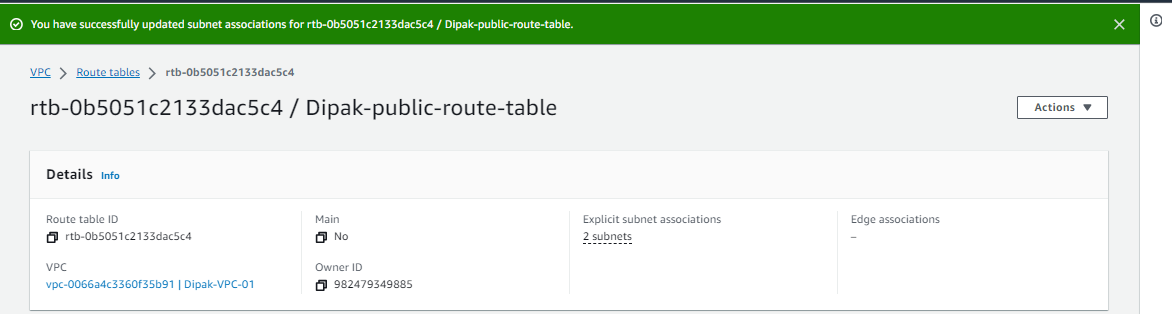


Figure 22 editing route table and adding internet gateway

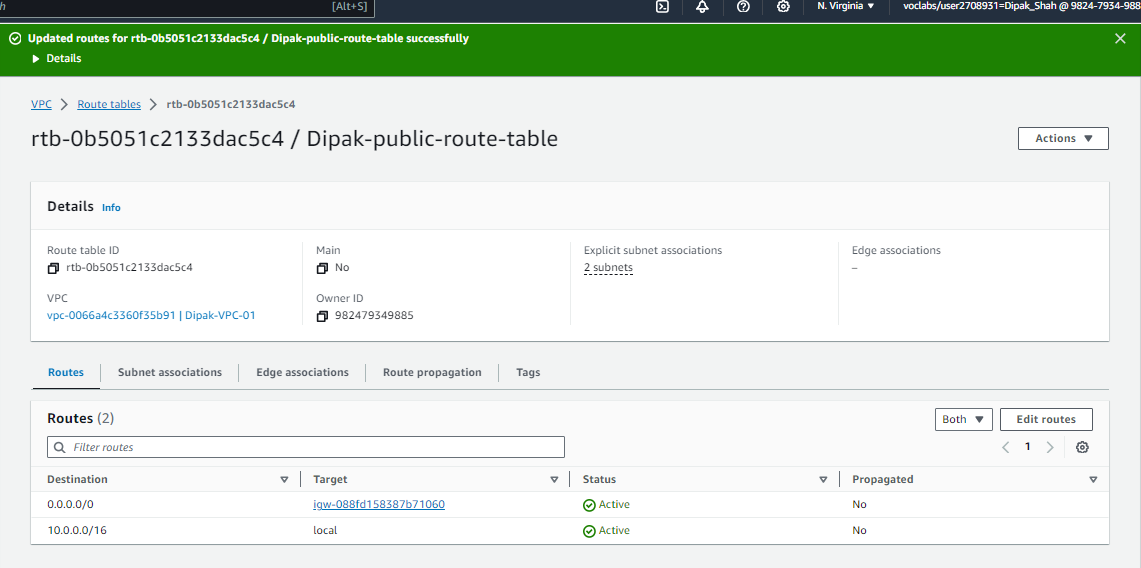


Figure 23 complete route table

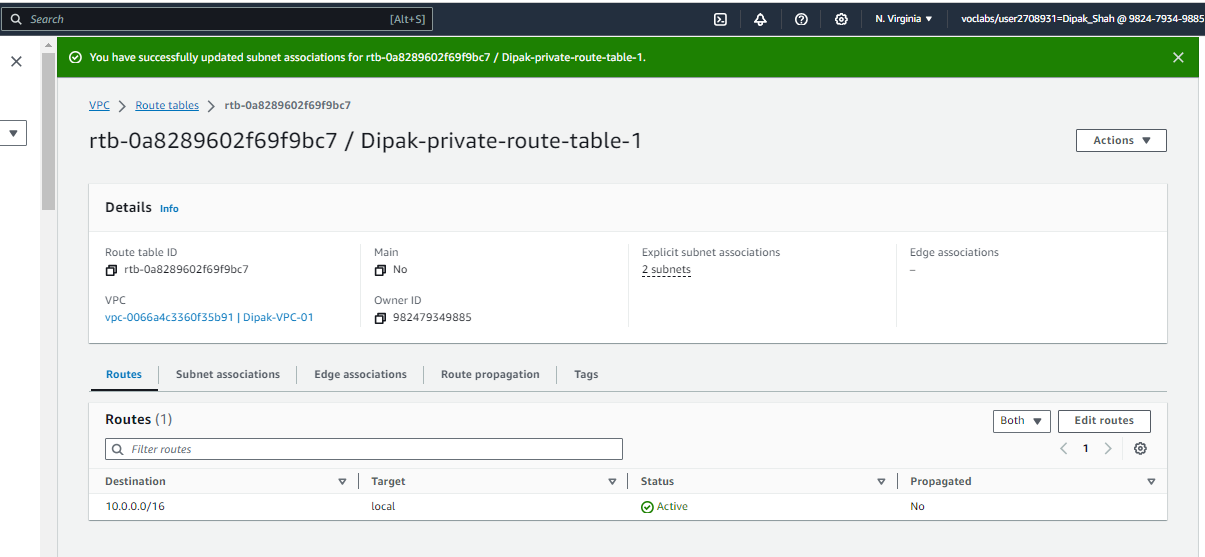
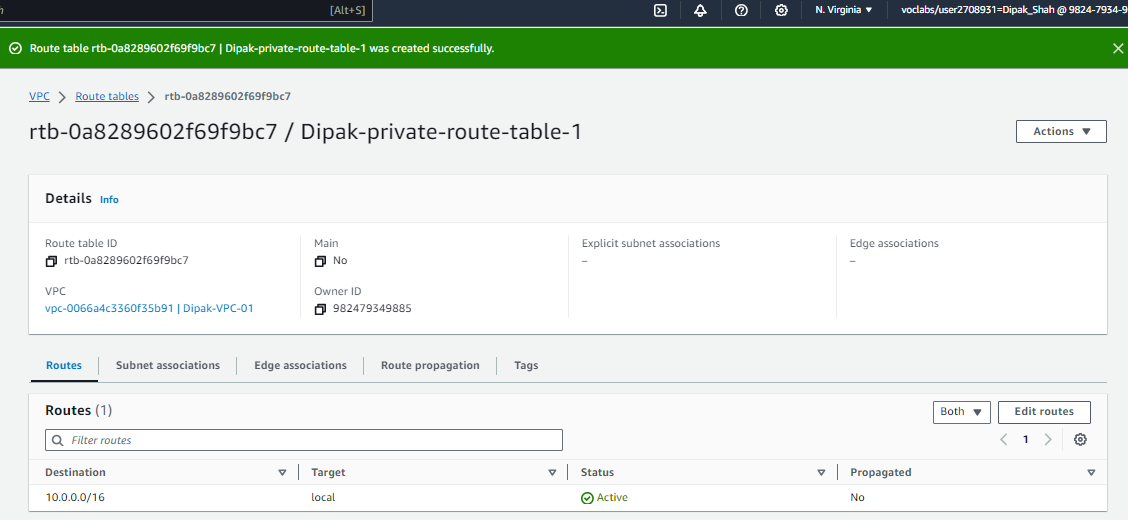


Figure 24 creating private route table



Figure 25 Adding NAT gateway

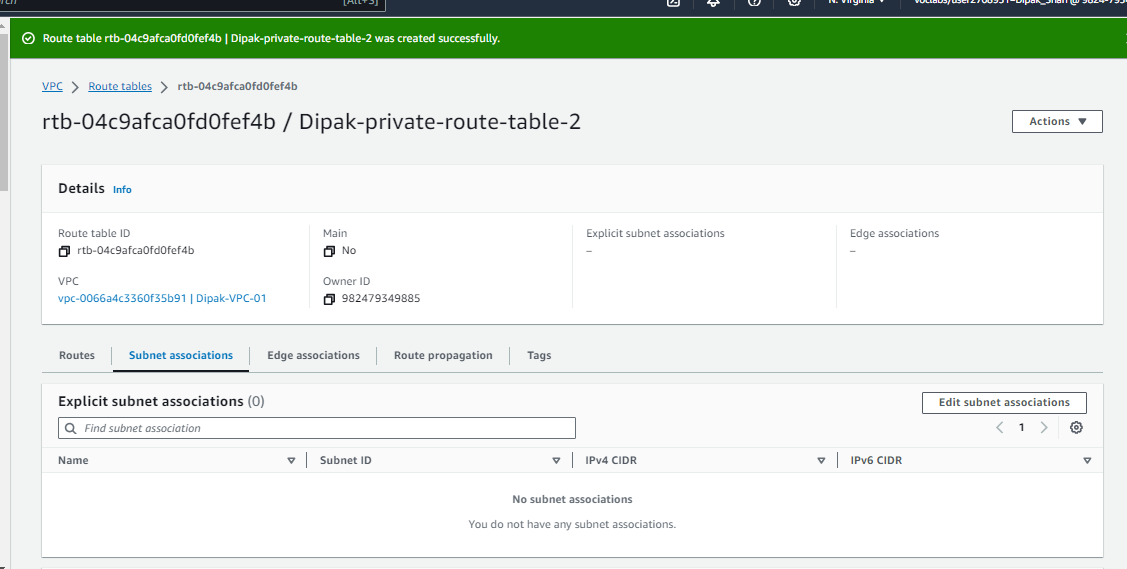
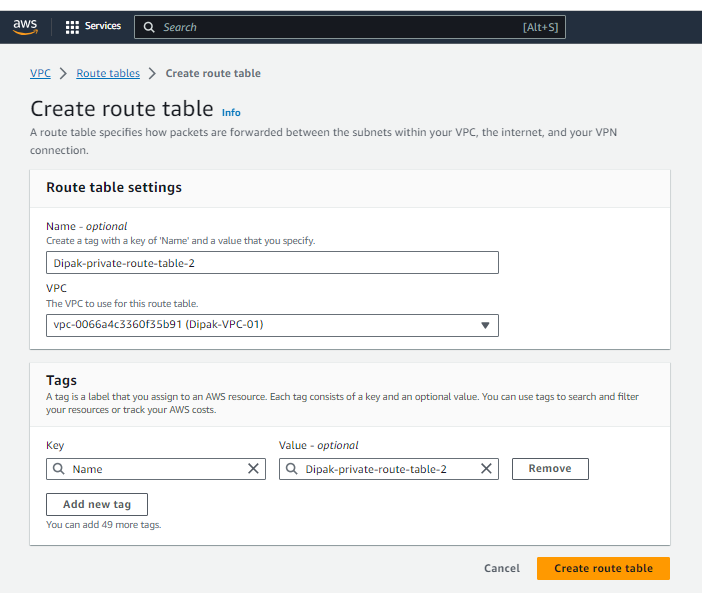
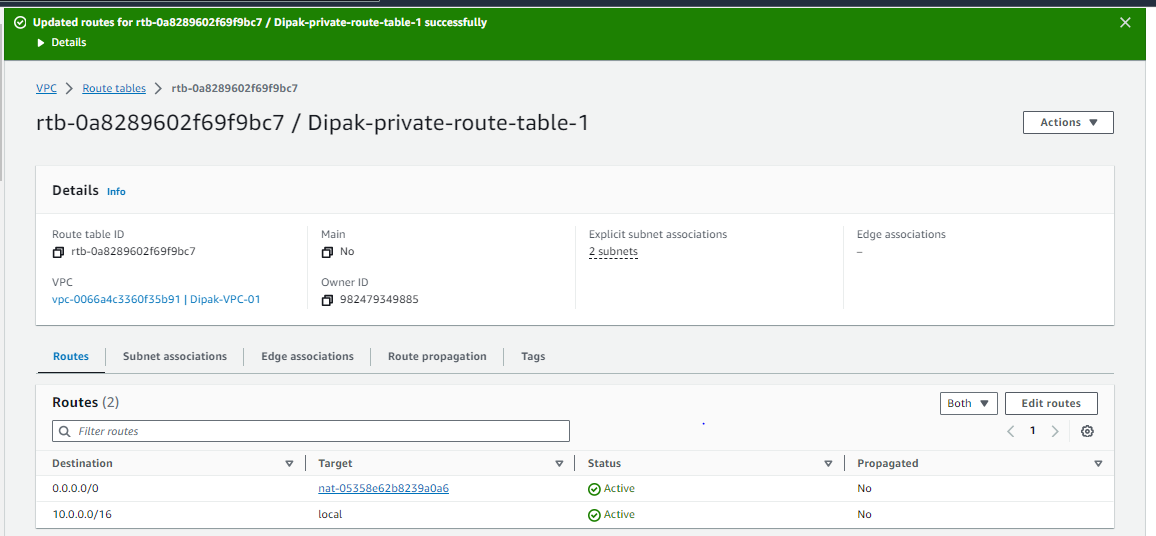
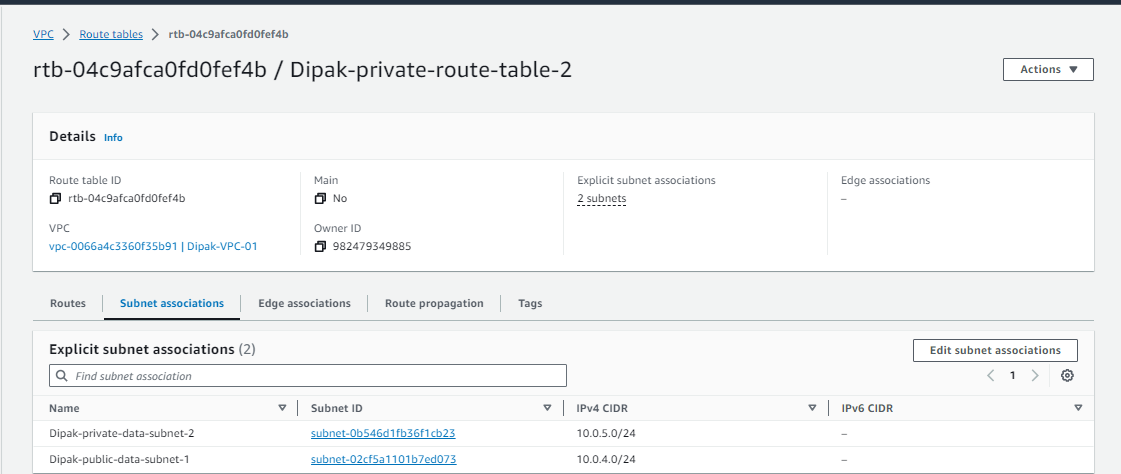
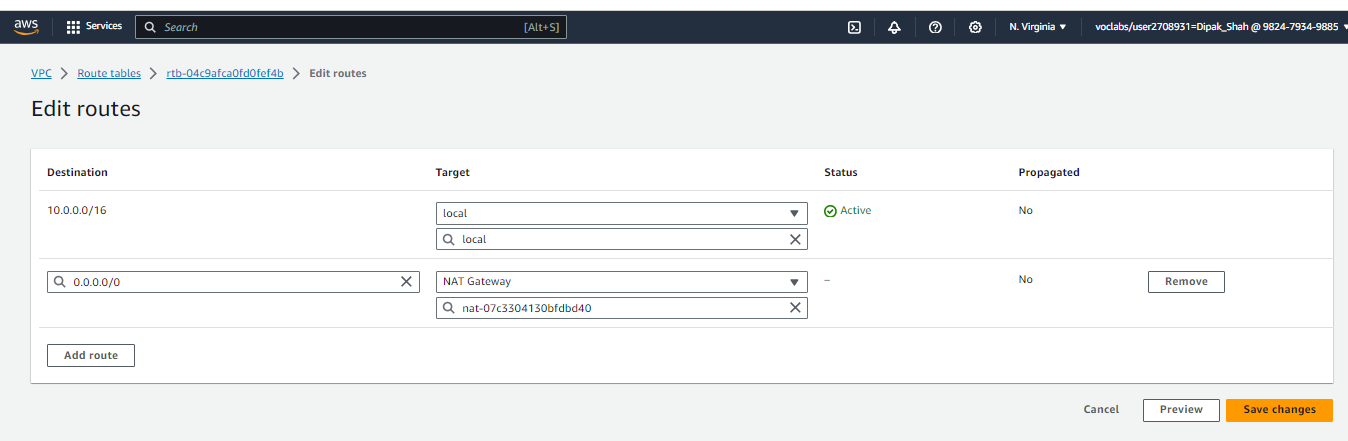
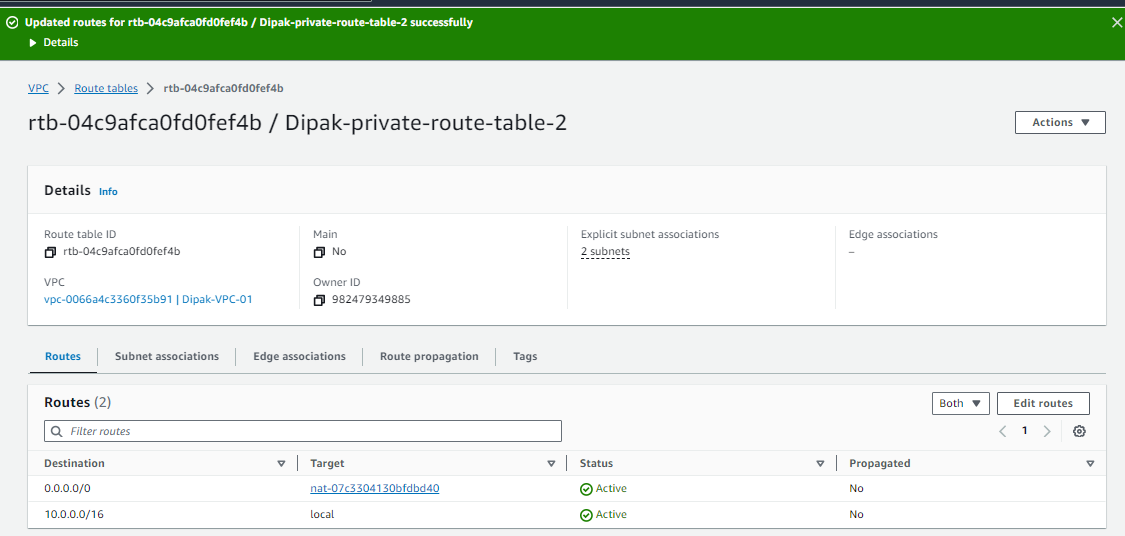


Figure 26 creating second private route table





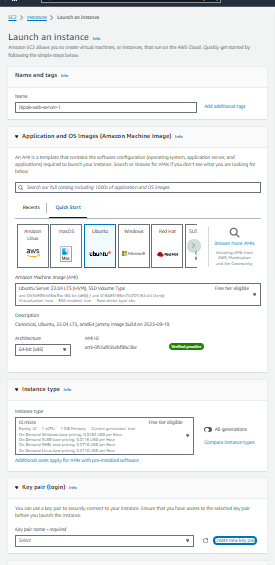
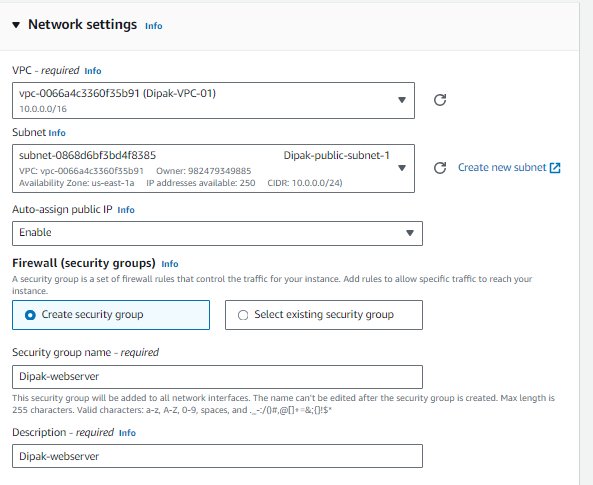
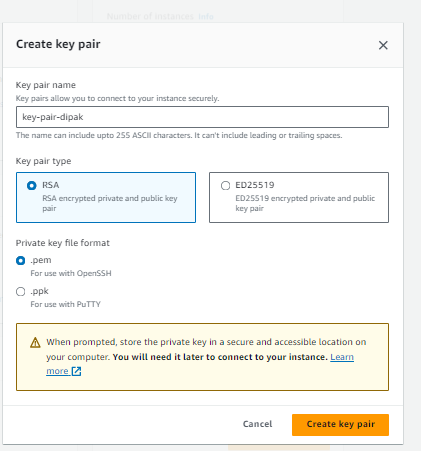
  


Figure 27 creating EC2

Figure 28 Creating key-pair

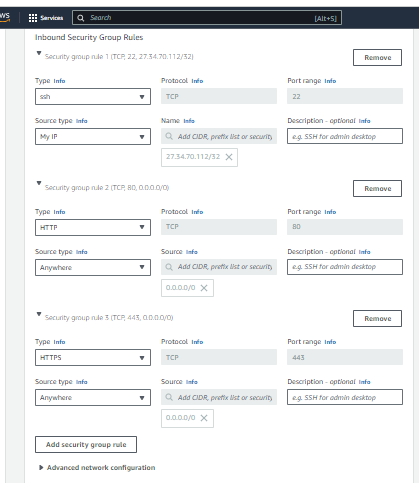


Figure 29 adding security

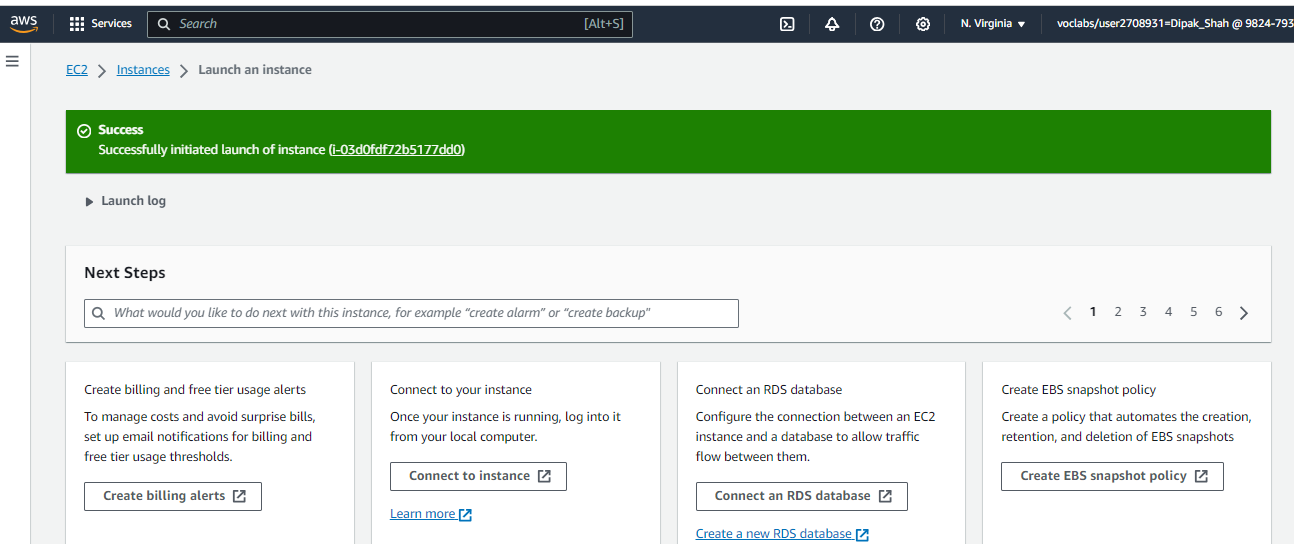


Figure 30 EC2 created successfully

# 

Figure 31 running from DNS

# 

Figure 32 using codes

# 

Figure 33 London college websites

# 

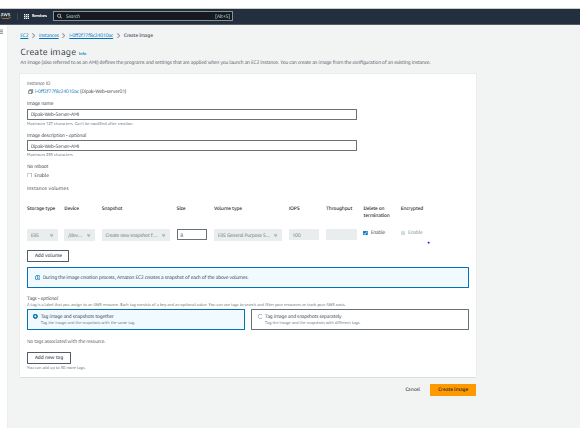
Figure 35 selecting instances

Figure 34 Creating image

# 

# 

Figure 36 adding target group

# 

Figure 37 selecting VPC

# 

Figure 38 creating target group

# 

Figure 39 creating Application Load Balancer

# 

Figure 40 selecting zones

# 

Figure 41 selecting target group

# 

Figure 42 summary of load balancer

# 

Figure 43 created load balancer successfully

# 

Figure 44 now creating launch template

# 

Figure 45 enable cloud monitor

# 

Figure 46 created load balancer successfully

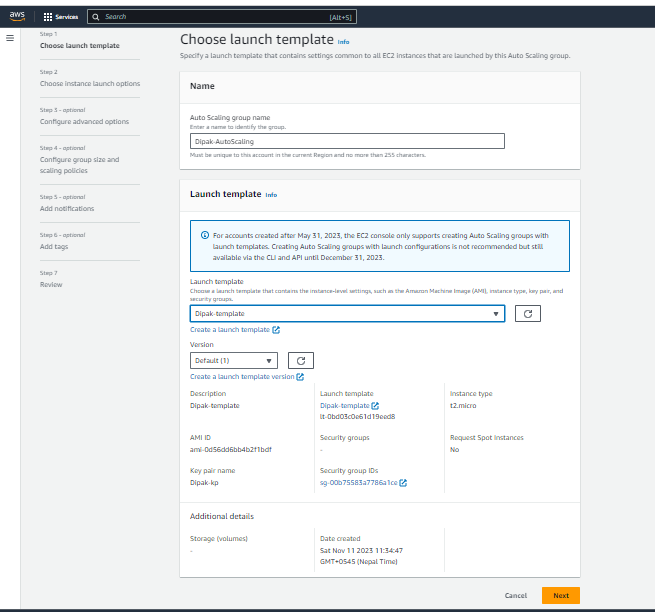


Figure 47 selecting lunch template

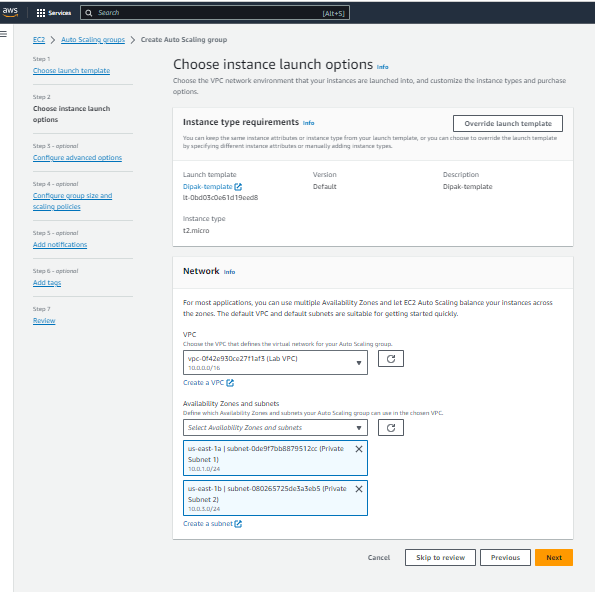


Figure 48 creating auto scaling groups

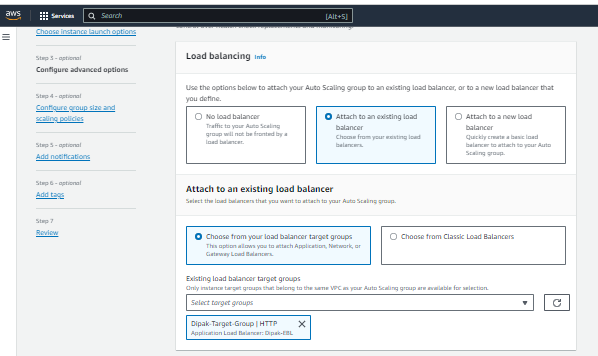


Figure 49 adding load balancing

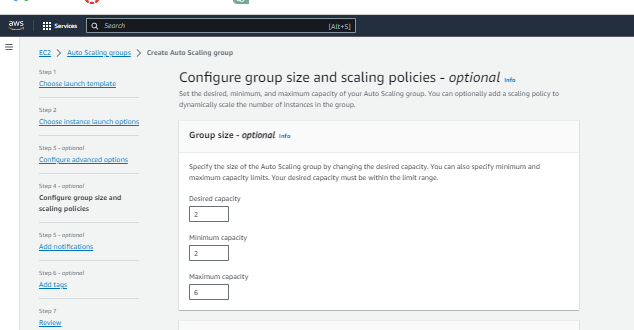
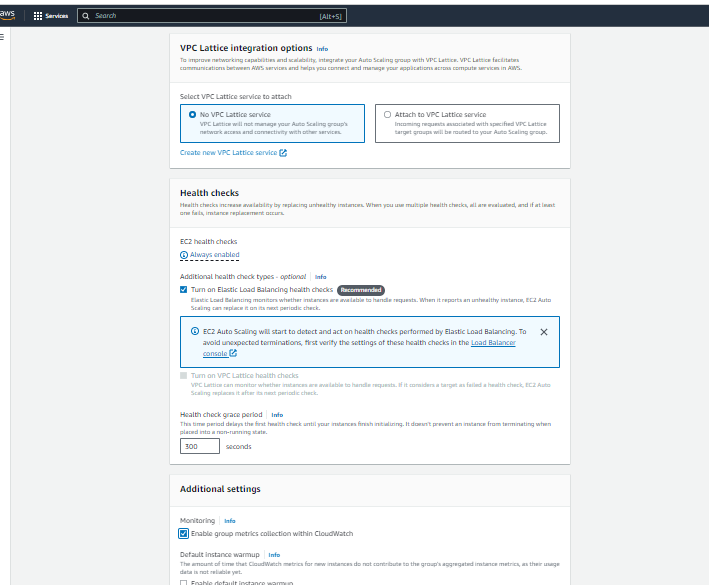


Figure 50 creating capacity

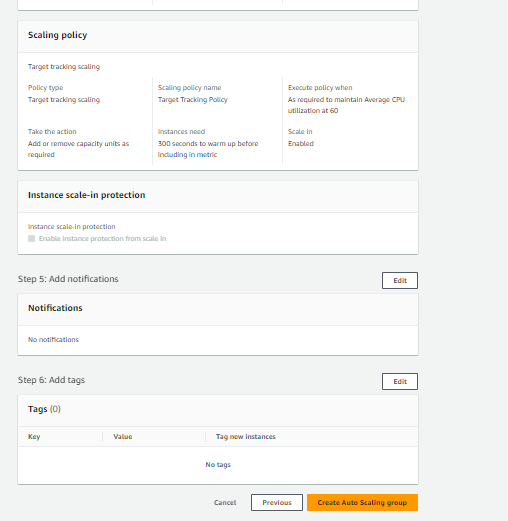
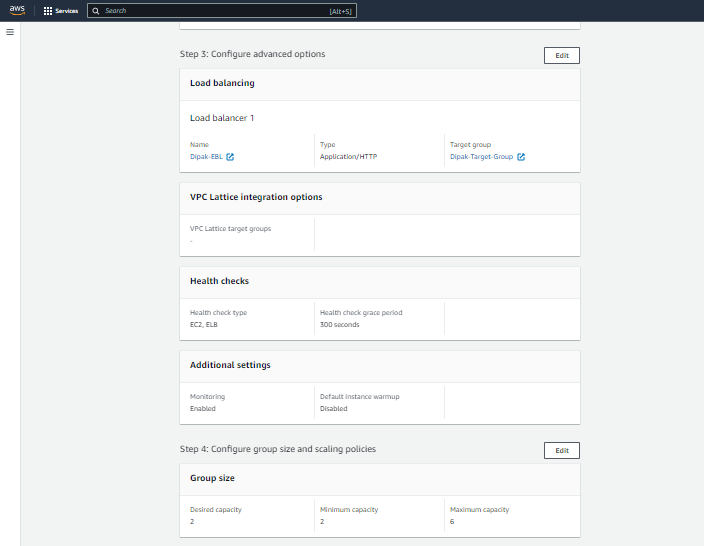
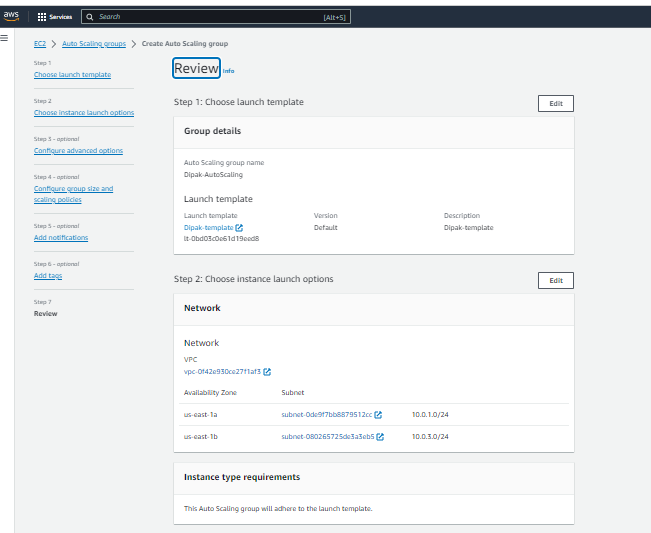
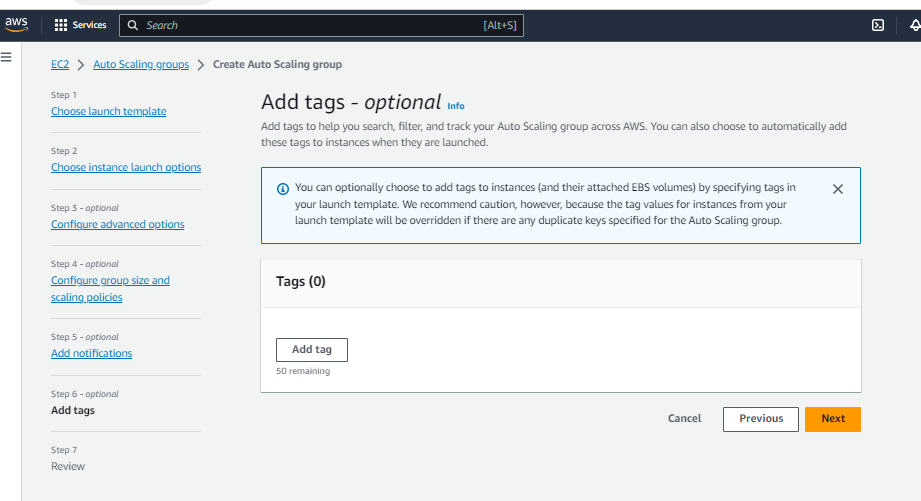
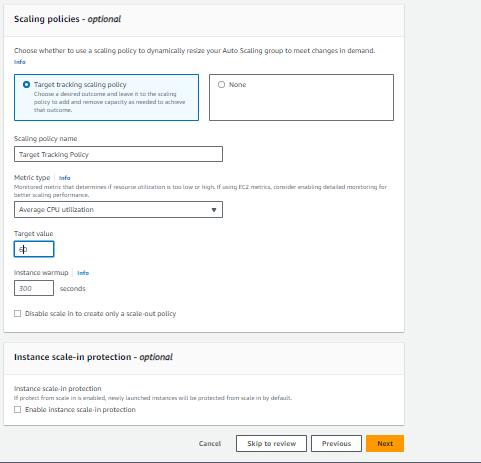


Figure 51 review everything and creating auto scaling

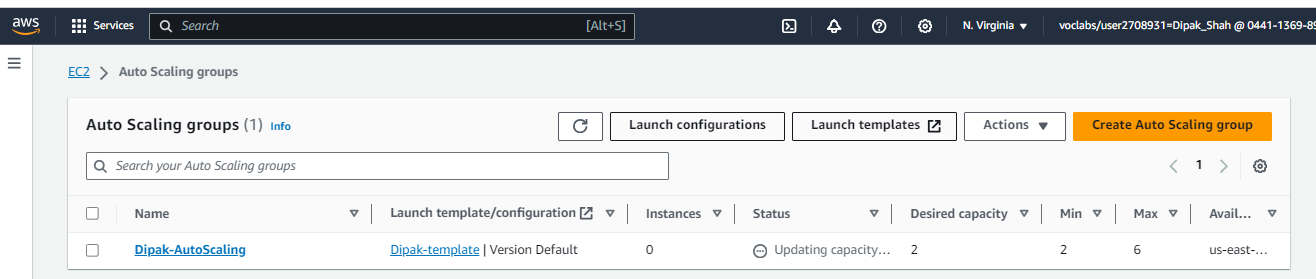


Figure 52 created auto scaling

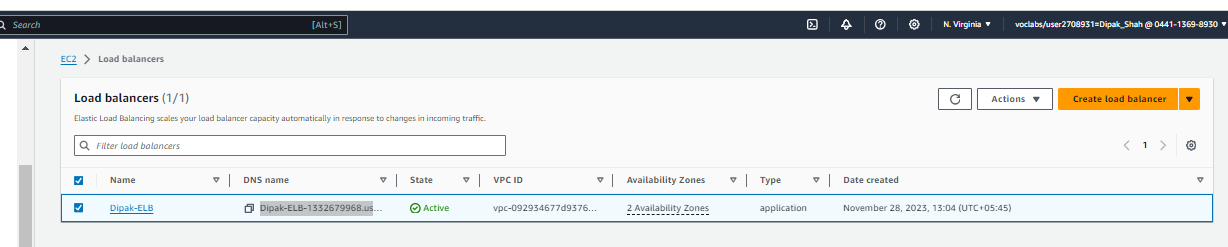


Figure 53 Copy DNS name to run cloud watch

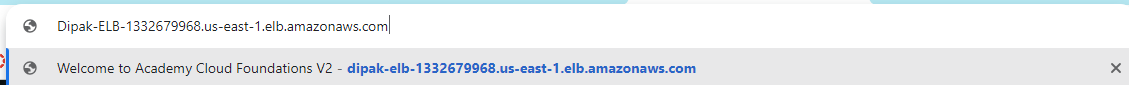


Figure 54 running website



Figure 55 current CPU load

# Implementing a Cloud Computing Platform using Open-Source Tools

In the context of Siddhartha Cloud Computing Pvt. Ltd. assisting The London College in migrating its on-premises services to the cloud, the focus would be on aligning the utilization of open-source tools and technologies with Siddhartha's cloud framework. Let's dive deeper into each phase:

# Selection of Open-Source Tools and Technologies

To this end, we select open source tools that fit into Siddhartha Cloud Computing Platform easily. Tools that can be used by Siddhartha include Kubernetes, Terraform, and Prometheus as long as they work well with the London College’s systems and cloud provision services.

The first stage where the focus will be on configuration, customization and tweaking of selected open source tools in Siddhartha’s Cloud framework during set up. The purpose of this process is to successfully mesh London College’s current system with Sidddartha’s cloud platform. Tightening of installation, calibrating configurations, and checking compatibilities for smooth changeover are considered here.

The deployment of a three-tier architecture uses open source components consistent with Siddhartha’s clouds. ``` For example, choosing Apache or NGINX for the front-end, middleware solutions like Node.js or Django and strong databases like MySQL or MongoDB for the data layer. In this focus, they are tailored to easily adapt and blend into Siddhartha’s Cloud Architecture.

Connectivity and load balancing within Siddhartha's cloud infrastructure are crucial for optimal performance. Siddhartha would configure tools like HAProxy or Kubernetes' load balancing features to ensure smooth connectivity and efficiently distribute incoming traffic across the cloud servers, optimizing resource utilization and ensuring high availability.

Siddhartha employs strong monitoring tools like Grafana, Prometheus, and ELK stack to properly supervise The London College’s cloud services. Siddhartha also makes use of other automation tools such as Ansible and Chef which help them manage their cloud infrastructure more efficiently.

Through this detailed process, Siddhartha’s open-source tools and technology will precisely match its infrastructure; making the process of moving The London College services to Siddhartha’s cloud more fluid.

# Potential Issues and Constraints

The London College's migration to Siddhartha Cloud Computing's platform, let's explore the potential issues and constraints that might arise during this process:

# Network Latency and Performance Challenges

Therefore, Siddhartha’s network may be hampered by such issues as network latency occasioned by geographic difference between LIPA building and Siddhartha data centers in Kathmandu. Application performance and user experience can also be affected by this. In doing so, Siddhartha should provide efficient networking solution, such as CDN/edge caching systems in order to reduce delays and improve response rate for the users of The London College.

# Data Security and Compliance Concerns

Transfer of the London College’s data to Siddhartha’s cloud creates issues of security and compliance. For data integrity purposes and compliancy with GDPR and HIPAA regulation, Siddhartha must provide evidence of comprehensive data encryption methods, access controls, etc. To solve these worries, The London College’ s IT security department should cooperate with a different security team in implementing extra security protocols as well as conducting routine audits.

# Cost Management and Budget Constraints

Siddhartha needs to consider the costs involved in his plan to migrate to the cloud. In order to maintain transparency he must have discussions, about pricing with The London College. Come up with a strategy that is cost effective and, within budget limits. His goal is to use approaches to make the use of resources optimize instance sizes and take advantage of affordable pricing plans. This way he can ensure that the migration process is both efficient and doesn't put a strain on finances.

# Training and Skill Gaps among IT Staff

The IT staff, at the London College might encounter difficulties, in managing and operating within the cloud environment provided by Siddhartha. To address this issue Siddhartha can offer training programs and detailed documentation to enhance the skills of the colleges IT team in utilizing the new cloud services. By organizing training sessions and workshops any skill gaps can be bridged, enabling the team to handle and sustain the cloud infrastructure.

# Vendor Lock-In and Portability Issues

There is a risk of vendor lock in if The London College becomes too dependent, on Siddhartha’s technologies or tools. To avoid this Siddhartha should prioritize interoperability and adherence to standards. Offering support for data portability, compatibility with cloud strategies and flexible contract terms can help address concerns, about being locked into a particular vendor.

Addressing these issues proactively and collaboratively between Siddhartha Cloud Computing and The London College is crucial to ensure a smooth migration, maintain performance standards, uphold data security, manage costs efficiently, bridge skill gaps, and prevent vendor lock-in during the transition to Siddhartha's cloud platform.

# Network Latency and Performance Challenges

These strategies have the goal of identifying, analyzing and addressing issues, by implementing actions or plans that are tailored to overcome the challenges that have been identified. They involve a combination of techniques, solutions and approaches that are designed to navigate obstacles and ensure a transition of services while minimizing disruptions and optimizing performance, security and cost-effectiveness.

# Challenges Related to Network Latency and Performance

Strategy; Hosting based on Proximity: To reduce latency it is recommended to deploy services from The London College to Siddhartha’s data centers. This can be achieved by utilizing Siddhartha’s distributed centers or leveraging edge computing techniques to minimize the time it takes for data to travel.

Solution; Content Caching and Integration with Content Delivery Networks (CDNs): To optimize content delivery and mitigate the impact of latency on user experience caching mechanisms should be implemented along with integration with Content Delivery Networks (CDNs). This allows for storing and delivering content closer, to end users.

# Addressing Data Security and Compliance Concerns

Approach; Securing Data Transmission and Storage: To ensure the safety of data, within Siddhartha’s cloud infrastructure we will implement end to end encryption for data transmission. Employ encryption methods for data storage. We will consistently. Update our encryption protocols to align with compliance standards.

Solution; Demonstrating Compliance Certifications and Transparency: We understand the importance of security standards so we will obtain compliance certifications like ISO and SOC 2 to showcase our commitment to adhering to these standards. Additionally we will provide transparency through audits to assure The London College about the security of their data and regulatory compliance.

# Managing Costs in Alignment with Budget Constraints

Approach; Optimizing Resources and Scaling: To effectively manage costs while maintaining performance we will implement automated resource optimization tools that continuously monitor resource allocation. By utilizing auto scaling features we can match resource provisioning with demand optimizing costs without compromising performance.

Solution; Analyzing Costs in Detail and Forecasting: We recognize the importance of aligning resources, with The London Colleges budget goals. To achieve this we will conduct cost analysis and forecasting exercises that identify savings opportunities. Regularly reviewing usage patterns allows us to adjust resource allocation accordingly based on constraints.

# Training and Skill Development Initiatives

The London College recognized the need to elevate its IT team's cloud expertise. Siddhartha developed a multi-pronged training strategy with tailored workshops focusing on migration tools and their cloud platform. Hands-on sessions along with detailed documentation sought to upskill staff. Collaborative work between experts and IT fostered knowledge sharing of best practices. Siddhartha's experts worked closely with the team, exchanging ideas in lengthy discussions and providing support during the complicated transition. Regular meetings maintained an open exchange, moving the modernization effort forward.

# Vendor Lock-In and Portability Issues

Network challenges, data security, and cost optimization are crucial concerns for any organization's cloud migration. By embracing open standards and hybrid cloud adoption, Siddhartha Cloud aims to address these issues and empower its customers. Their solutions focus on interoperability, portability, and flexibility. Data and workloads can seamlessly integrate between on-premises infrastructure and Siddhartha's cloud services. This hybrid approach reduces dependency on any single vendor by allowing some services to remain locally hosted. Moreover, implementing open standards facilitates easy migration between cloud providers and ensures customers retain control over their data.

Overall, Siddhartha Cloud's strategy prioritizes customer empowerment, security, and choice above vendor lock-in. Their solutions aim to offer a tailored approach for a successful migration and sustained performance throughout The London College's digital transformation.

# Conclusion

The technical report delves into configuring cloud computing platforms using both AWS and open-source tools. It outlines setting up AWS components like VPCs, NAT gateways, security groups and auto-scaling mechanisms. These robust capabilities enable customized cloud infrastructure. By implementing versatile open-source tools across architectural layers, their adaptability is showcased. Addressing challenges involving network latency, security compliance, budget constraints and skill shortages culminates in strategic mitigation approaches. Overall, a comprehensive guide illustrating AWS and open-source tool prowess provides strategic insights to optimize cloud migration benefits while navigating complexities. Skilled development and vendor concerns require attention to ensure smooth transitions.

# Part-3

# Introduction

Cloud computing has become very important changing how people store, process, and access data. This article tries to uncover the increasing significance of cloud computing on current day’s life styles which impact various fields. We focus on shedding light on security and data protection issues that are connected with adopting such technology in order to prove how significant it is to study them. Moreover, this paper looks at how clouds computing can be used efficiently and ways of preventing security breaches as well as protection of information. This provides room for cloud computing discussion as well pointing to security and data protection challenges associated with it.

# Purpose of article

This article will try to explore the tricky terrain of cloud computing as far as security and data are concerned. Addressing these issues enables businesses, persons, and technology owners to understand how to reduce risks as well as exploit secure ways of using cloud services appropriately. This article also tries to emphasize on preventative actions and good practice in order to protect critical information, thus making businesses operate with awareness while embracing cloud operations.

# Scope of article

This manuscript focuses on some common failures/weaknesses, security problems, and data privacy challenges faced by many of today’s cloud based systems or infrastructures. Data security in multi-tenancy; an issue encompassing hacking, breach of data, complexity of regulations, and the nuances surrounding information privacy within a common framework. Additionally, this overview outlines the breadth of potential risks and exposures associated with cloud adoption by both organizational entities and their end users as well.

# Common Problems in Cloud Computing

There are various common complications associated with use of clouds by companies which are commonly referred to as recurrent challenges for cloud computing. Such challenges concern the scalability of adjusting resources appropriately, problems with unavailability caused by reboots that result in unavailable services which affect accessibility, concerns about possible data loss, high costs involved, as well as issues associated with vendor lock-in and the limitations when it comes Therefore, resolving these concerns will help organization ensure that their processes are dependable, safe, and affordable. Some of these problems are addressed by developing strategies as well as implementing creative solutions geared towards improving cloud computing systems’ resilience and performance. Here’s a detailed exploration of common problems in cloud computing along with future-oriented solutions:

# Scalability Challenges

Scalability problems are mostly determined by resource adaptation to unpredictable demand changes. Automated Scaling will be enabled in the future due to advances in scalable predictive analytics and associated AI. The seamless scaling of the resources should be supported by machine-learning algorithms that would predict spikes in demand and adjust the resources automatically.

* **Downtime and Service Disruptions**

They also help companies avoid some downtime during anticipation of the future in fault-tolerant architectures. Real time analytics would forewarn probable breakdowns allowing active mitigation measures to forestall service disturbances. Uninterrupted services during outage will be possible because of decentralized systems and edge computing thereby increasing overall reliability.

# Data Loss and Recovery

The future of data protection is being shaped by innovative strategies. Data will be protected through block chain-based encryption and decentralized storage. AI-based anomaly detection would allow for easy identification of problems as well as data recovery.

# Cost Management and Overspending

Expenditure management is set to take a new twist with AI power cost optimization tools in the near future. Predictive cost analytics, as it predicts requirements, will mitigate against over provision. Rightsizing through automation will lead to more efficient utilization of resources resulting into significant cost cuttings.

# Vendor Lock-In and Portability

Interoperability standards and open-source platforms will dominate the future cloud landscape. Multi-cloud strategies will thrive, facilitating seamless migration between vendors. Containerization technologies and standardized APIs will ensure portability, empowering users to circumvent vendor lock-in.

# The Most Common Cloud Computing Problems and their Solutions

The future will witness a strong ecosystem composed of predictive analytics, AI driven automation, decentralized architecture, and interoperable standard. If implemented correctly, these solutions would go a long way in addressing some of the most common problems with cloud computing such as improved performance, security, and scalability.

# Contemporary Security Issues in the Cloud

Contemporary security troubles inside the cloud talk over with the evolving challenges and vulnerabilities confronted via agencies using cloud computing services inside the gift technological landscape. These problems encompass more than a few concerns, which includes information breaches, unauthorized get right of entry to, inadequate identification and access management, insider threats, statistics leakage, compliance and regulatory troubles particular to cloud environments. Addressing these current challenges includes deploying superior security measures, adopting sturdy encryption strategies, enforcing stringent get right of entry to controls, leveraging AI-pushed monitoring for anomaly detection, and ensuring compliance with evolving regulations to safeguard sensitive records and keep the integrity and protection of cloud-primarily based operations. Our cloud migration project for The London College, understanding and mitigating contemporary security concerns are paramount.

# Data Breaches and Unauthorized Access

Data Threats Data is considered to be one the most important valuable resource of any organization and the number of customers shifting their data to cloud is increasing every day. Data life cycle in cloud comprises of data creation, transit, execution, storage and destruction. Data may be created in client or server in cloud, transferred in cloud through network and stored in cloud storage. When required data is shifted to execution environment where it can be processed. Data can be deleted by its owner to complete its destruction. The biggest challenge in achieving cloud computing security is to keep data secure.

# Data loose

The clients can lose the control over information in distributed computing due to the outsider models of the cloud. The information, applications, and assets are situated with the supplier; the client personality administration is taken care of by the cloud; and the client get to control rules, security strategies, and requirement are overseen by the cloud supplier. The purchaser needs to depend on the cloud supplier for information security and protection, and accessibility, and checking and repairing of administrations or assets.

# Inadequate Identity and Access Management

Enhancing identity and access management with biometric authentication and context-based controls will be pivotal. By implementing adaptive access controls and dynamic authorization based on user behavior, we aim to prevent potential security gaps during user access transitions to the cloud environment.

# Insider Threats and Data Leakage

Leveraging AI-driven monitoring tools during the migration process will help detect anomalies in user behavior. Deploying robust data loss prevention (DLP) mechanisms and encryption protocols will mitigate potential risks from insider threats, safeguarding sensitive data during the transition phase.

# Strategies for Addressing Current Cloud Security Issues:

Our approach is multifaceted, combining regular security audits, constant employee training on cloud security best practices, and tight coordination with the chosen cloud service provider. Staying up to speed on security updates and configuration reviews will protect our cloud environment from evolving threats, guaranteeing a secure migration process for The London College's data and services.

# Building a Secured Cloud Computing Platform

Securing the cloud environment against malicious and intelligent hackers is a process that calls for comprehensive efforts to harden the architecture against ever new breeds of threats and safeguard confidential information. Every aspect is very important in building a strong defense framework on the cloud, risk reduction, and upholding the credibility and safety of the work done.

# Identity and Access Management Best Practices

Strong IAM policies comprise of MFA, RBAC, and minimal privilege principles. The next step will comprise of utilizing biometric authentication and adaptive access controls so that only those who are supposed to get access will obtain it and AI-based behavioral analytics that constantly change as the attackers’ tactics evolve.

# Data Encryption and Tokenization

It is important to encrypt data and tokenize in order to secure sensitive information. Leveraging AES-256 encryption and homomorphic encryption can strengthen data security. To tokenize sensitive data in the cloud environment is to ensure confidential treatment of these data, as well as their integrity.

# Continuous Monitoring and Threat Detection

Threat identification in real time must involve continuous monitoring, and proactive threat detection systems. The platform will use artificial intelligence and machine learning models in order to identify and respond to anomalies quickly. The platform’s resistance to changing threats will be improved through intrusion detection systems (IDS) and behavior-based anomaly detection.

# Compliance and Auditing Solutions

Audit and compliance should be strong for ensuring conformity to legal regulations. Automated compliance checks using block chain technology with immutable audit trail, and artificial intelligence based compliance tools will make the process smoother with compliance with various legal regimes. The real-time compliance will be continuously monitored by using these compliance metrics.

# Employee Training and Security Awareness

Adopt employee-oriented and extensive training programmers that promote security conscious culture. The staff will participate in regular cybersecurity awareness sessions and simulated phishing exercises to understand emerging threats as well as best practices against them. This enables the platform’s employees to identify some of the security issues to ensure that the system is secure.

Combining all this, a strong and secure cloud computing system is created. Strong IAM practices, encryption protocols, continuous monitoring and threat detection, compliance, and a culture of security awareness, all combined underpin the infrastructure, protecting it against risks that are inherent in cloud computing. These elements together aim at creating data security i.e., the cloud technology requires that the data should be confidential, intact, and available anytime for business purposes.

# Data Protection During Cloud Migration

One of the critical issues revolving around data migration into cloud-based services entails data security or protection. For the purpose of protection of the info, organizations need to first categorize and stock take their information, separating sensitive and non-confidential information. The first stage acts as an underpinning point that allows the implementation of the relevant security aspects that can be supported by information on hand.

# Understanding Data Classification and Sensitivity

Data classification refers to classifying of a data depending upon their degree of sensitivity as well as significance. The next step involves understanding what kind of data is being migrated; for instance, this might include PII, financial records, intellectual properties and other normal sensitive data. Organizations are able to determine which organization, group or specific individual gains access to any particular piece of sensitive information by classifying it. Knowing what kind of information it is helps you figure out what precautions to take when moving it and which safeguards are necessary.

# Data Encryption and Secure Transfer

Encrypting information, whether at rest or while being transmitted can ensure that it cannot be accessed by third parties, thereby enhancing privacy. Robust encryption systems like AES-256 encryption ensure unencrypted data is safe when kept on the cloud. Also, employing the safe communicator protocol such as TLS/SSL when transferring data from on-site system to the cloud also helps in protecting the data all along the way.

# Backup and Disaster Recovery Planning

It is essential for organizations to come up with an extensive system of backups and disaster recovery to avoid data loss while in transit. Provides redundancy by making a multiple backup of data before and during migrations against possible bugs. Using backup plans and resilient storage technologies ensures that the stored data is accessible after events which are difficult to predict.

# Legal and Regulatory Compliance

In particular, respecting the law in terms of information privacy is fundamental for all organizations. Organizations should insist that a cloud service provider comply with a standard e.g., GDPR/HIPAA/industry specific standards. Data mapping involves making sure that the cloud provider complies with contractual obligations and various compliance requirements so as to reduce legal risk and ensure security.

# Creating a Data Protection Strategy for the London College.

Combination of different security approaches and strategies is needed for tailoring a data protection policy especially for The College of London. This involves performing an in-depth risk analysis on the sensitivity of the data; use of strong encryption techniques; provision of secure transportation alternatives for the information; formulating an effective disaster recovery strategy; conforming with applicable laws; as well as frequent review and update of current security mechanisms based on latest data protection strategies. Through persistently exercising these extensive data security measures, institutions can have a hassle free movement into the cloud and guarantee safety of the information assets’ sensitive nature, integrity, and accessibility.

# Conclusion

Such a transition entails many challenges besides other important security aspects that require to be well understood. The scale challenges, in terms of possible downtime, loss of data, cost management and compliance complexity, demonstrate the many dimensions of maintaining a secure cloud platform. These complexities indicate that, to tackle such issues, strong security provisions must be put in place. The following are some of key recommendation to strengthen the security mechanism and reduce the risk in the migration processes under these circumstances. Some of the major components of these recommendations includes strengthening of proper identification and control mechanism, inclusion of up-to-date encryptions procedures and constant monitoring. Moreover, it is imperative to come up with specific security classifications which include encrypting data while it’s in storage or being transmitted for safety measures. This is accompanied by developing a reliable plan when the need arises for backups and disaster recovery purposes.

To successfully migrate the London College’s data with respect to the integrity and privacy, it’s important to execute the above recommendations carefully. This implies complete data categorization to identify personal details, intensive encrypting of vital information, and robust disaster recovery processes. Moreover, it should be possible to follow the rules concerning various aspects of law, including those related to safety at work, environmental protection, etc., which will prevent possible law suits. Security is critical in migration of all services into the cloud. Consequently, this exercise should be undertaken with caution and holistically. Acknowledgement of common issues, adherence to essential recommendations and crafting of appropriate strategies for protection of London College’s data in a resilient and secure cloud environment. Through this strategy, data is well preserved, ensuring that the rules are followed in the cloud as the institution transact digitally.

# Reference

1. (No date a) *What is cloud computing - aws.amazon.com*. Available at: https://aws.amazon.com/what-is-cloud-computing/ (Accessed: 22 November 2023).
2. (No date b) *IEEE Xplore | IEEE Journals & Magazine | IEEE Xplore*. Available at: https://ieeexplore.ieee.org/abstract/document/7876843/ (Accessed: 22 November 2023).
3. Boisvert, M., Bigelow, S.J. and Chai, W. (2022) *What is iaas? infrastructure as a service definition: TechTarget*, *Cloud Computing*. Available at: https://www.techtarget.com/searchcloudcomputing/definition/Infrastructure-as-a-Service-IaaS (Accessed: 22 November 2023).
4. *What is ...* (1978) *Amazon*. Available at: https://aws.amazon.com/what-is/cloud-storage/ (Accessed: 22 November 2023).
5. *What is Paas?  |  google cloud* (no date) *Google*. Available at: https://cloud.google.com/learn/what-is-paas (Accessed: 22 November 2023).
6. (No date a) *Cloud computing: Issues and challenges - IEEE xplore*. Available at: https://ieeexplore.ieee.org/abstract/document/5474674 (Accessed: 22 November 2023).
7. (No date b) *Disaster recovery in cloud computing systems: An overview*. Available at: http://irep.iium.edu.my/83396/13/83396\_Disaster%20recovery%20in%20cloud%20computing%20systems.pdf (Accessed: 22 November 2023).
8. (No date c) *Cloud computing: Issues and challenges - IEEE xplore*. Available at: https://ieeexplore.ieee.org/abstract/document/5474674 (Accessed: 22 November 2023).
9. Calzon, B. (2023) *Learn the top cloud computing challenges, risks & issues*, *datapine*. Available at: https://www.datapine.com/blog/cloud-computing-risks-and-challenges/ (Accessed: 22 November 2023).
10. Grant, M. (no date) *Software as a service (SAAS): Definition and examples*, *Investopedia*. Available at: https://www.investopedia.com/terms/s/software-as-a-service-saas.asp#:~:text=Software%20as%20a%20Service%20(SaaS)%20is%20a%20software%20licensing%20model,software%20on%20the%20user’s%20computer. (Accessed: 22 November 2023).
11. (No date a) *Overcoming challenges in cloud computing: TIPS and strategies*. Available at: https://www.ironhack.com/us/blog/overcoming-challenges-in-cloud-computing-tips-and-strategies (Accessed: 22 November 2023).
12. (No date b) *Overcoming challenges in cloud computing: TIPS and strategies*. Available at: https://www.ironhack.com/us/blog/overcoming-challenges-in-cloud-computing-tips-and-strategies (Accessed: 22 November 2023).
13. Calzon, B. (2023) *Learn the top cloud computing challenges, risks & issues*, *datapine*. Available at: https://www.datapine.com/blog/cloud-computing-risks-and-challenges/ (Accessed: 22 November 2023).
14. Kenlon, S. (no date) *5 open source tools for developing on the cloud*, *Opensource.com*. Available at: https://opensource.com/article/22/4/open-source-tools-developing-cloud (Accessed: 22 November 2023).
15. *VPC: Validación Periódica de La Colegiación* (2016) *Amazon*. Available at: https://docs.aws.amazon.com/vpc/latest/userguide/how-it-works.html (Accessed: 22 November 2023).
16. *What is cloud computing?  |  google cloud* (no date) *Google*. Available at: https://cloud.google.com/learn/what-is-cloud-computing#What%20Are%20The%20Types%20of%20Cloud%20Computing%20Services? (Accessed: 22 November 2023).
17. (No date a) *Introduction to the architecture framework | IBM cloud docs*. Available at: https://cloud.ibm.com/docs/architecture-framework?topic=architecture-framework-intro (Accessed: 22 November 2023).
18. (No date b) *Full article: Technologies, infrastructures and migrations: Material ...* Available at: https://www.tandfonline.com/doi/full/10.1080/13621025.2020.1784636 (Accessed: 22 November 2023).
19. Anton.gorbachev@clearscale.com (2023) *8 reasons to migrate to the cloud in 2023*, *https://blog.clearscale.com*. Available at: https://blog.clearscale.com/8-reasons-to-migrate-to-cloud-in-2020/ (Accessed: 22 November 2023).
20. Author (2022) *Cloud deployment models and real-time use cases*, *Payoda*. Available at: https://www.payoda.com/cloud-deployment-models-and-real-time-use-cases/ (Accessed: 22 November 2023).
21. BB Agency, info@bb. agency and Slingerland, C. (2023) *15 best cloud computing tools (updated 2023)*, *CloudZero*. Available at: https://www.cloudzero.com/blog/cloud-computing-tools/ (Accessed: 22 November 2023).
22. *Cloud deployment models* (2023) *GeeksforGeeks*. Available at: https://www.geeksforgeeks.org/cloud-deployment-models/ (Accessed: 22 November 2023).
23. Neal (2023) *Fundamentals of cloud computing*, *Digital Cloud Training*. Available at: https://digitalcloud.training/fundamentals-of-cloud-computing/#:~:text=Fundamentals%20of%20Cloud%20Computing%201%20%231%20On-demand%20Self-Service,Pricing%20...%205%20%235%20Broad%20Network%20Access%20 (Accessed: 22 November 2023).