

**Cloud Computing Security**

**Case Study - Proposal**

**Submission**

**SCHOOL OF INFORMATICS & IT**

**Case Study Group Report**

Student Name (Matric Number) : Mathanraj s/o Paneerselvam

C Aajith Kumar

Chan Yong Hoow

Tutorial Group : 1

Jenny LING (TP)

Tutor : Mr Eugene Swee Heng

Submission Date : 08 Jun 2025

**Declaration of Originality**

I am the originator of this work, and I have appropriately acknowledged all other original sources used as my references for this work.

I understand that Plagiarism is the act of taking and using the whole or any part of another person’s work, including work generated by AI, and presenting it as my own.

I understand that Plagiarism is an academic offence

and if I am found to have committed or abetted the offence of plagiarism in relation to this submitted work, disciplinary action will be enforced.

**Note to Tutor: This page is only to be used if your subject specifically allows AI-generated content to be used. Please delete this page if it is not required.**

**Declaration on the use of Generative AI tools for assignments**

|  |
| --- |
| Describe how you have used Generative AI tools such as ChatGPT or Dall.E-2 in your assignment.  Show snapshots of the conversations with the AI tool (i.e., the prompts you used and the response you get from the AI tool). |
|  |
| How do you indicate the reference?  The content generated by AI tools are not retrievable except by the user who generated them, so they are considered non-recoverable sources. Although non-recoverable data or quotations in APA Style papers are usually cited as personal communications, with ChatGPT-generated text there is no person communicating. Quoting text from ChatGPT chat is therefore more like sharing the output of an algorithm, with a reference list entry and the corresponding in-text citation.  According to the official APA Style site, ChatGPT references should be cited as:  E.g. OpenAI. (2023). *ChatGPT* (Sep 25 version) [Large language model].  <https://chat.openai.com/chat> |

**Important Note:**

* Do not copy answers produced by the AI tool in totality as it is considered as plagiarism.
* Do not rely on any information produced by the AI tool blindly. You should always verify the answer with other sources. Do not assume that these answers provided by the AI tool are correct.
* To achieve quality outputs from the AI tool, you should provide good prompt that is clear and specific. Be precise and provide context. Avoid asking open-ended questions.

Contents

[**Declaration of Originality** 2](#_Toc200328850)

[**Task 1 Network Architecture Diagram** 5](#_Toc200328851)

[**Contributions** 5](#_Toc200328852)

[**Reasons behind the architecture design** 5](#_Toc200328853)

[Transit Gateway 5](#_Toc200328854)

[Route 53 6](#_Toc200328855)

[High Availability 6](#_Toc200328856)

[High Performance 6](#_Toc200328857)

[**Task 2A** 7](#_Toc200328858)

[Advantages of AWS 7](#_Toc200328859)

[Disadvantages of AWS 8](#_Toc200328860)

[**Task 2B** 8](#_Toc200328861)

[1. Compromised Access Credentials: 9](#_Toc200328862)

[2. Misconfigured S3 Buckets: 9](#_Toc200328863)

[3. Excessive IAM Permissions: 9](#_Toc200328864)

[4. Insecure APIs: 10](#_Toc200328865)

[5. Insufficient Logging and Monitoring: 10](#_Toc200328866)

[**Task 2C** 10](#_Toc200328867)

[Phase 1: Assessment and Planning (Weeks 1-4) 10](#_Toc200328868)

[Phase 2: AWS Setup and Migration (Weeks 5-12) 12](#_Toc200328869)

[Phase 3: On-Premises Setup and Integration (Weeks 13-20) 12](#_Toc200328870)

[Phase 4: Optimization and Maintenance (After Week 20) 13](#_Toc200328871)

[Estimated Costs (CAPEX and OPEX) 13](#_Toc200328872)

[**Conclusion** 14](#_Toc200328873)

# **Task 1 Network Architecture Diagram**

## **Contributions**

The design of this network architecture is contributed equally by ideas from all the members of group.

For the individual parts of the report, the contributions are as follows:

Task 2A – Mathanraj s/o Paneerselvam

Task 2B – C Aajith Kumar

Task 2C – Chan Yong Hoow

We propose the following architecture design consisting of both AWS and on-premises solution to achieve high performance and high availability. We also included services to address migrating data from on-premises infrastructure to the cloud.

**A diagram of a cloud

AI-generated content may be incorrect.**

## **Reasons behind the architecture design**

The design needs to provide high performance and high availability as well as addressing migration of data from on-premises existing infrastructure to the AWS cloud. We have selected the components as below:

### Transit Gateway

The AWS virtual private cloud, on-premises networks (via Direct Connect or VPN gateway), and AWS services are all connected by the AWS Transit Gateway.

AWS Transit Gateway serves as a centralized gateway that links numerous Virtual Private Clouds (VPCs) and on-premises networks, making the transition from on-premises networks to the AWS cloud easier. It simplifies traffic routing and network administration, increasing the effectiveness and lowering the complexity of the integration process.

The advantages of using Transit Gateway are:

Scalable: Links on-premises networks and any number of VPCs.

Centralized: route management makes routing easier.

High Throughput: Facilitates data transmissions with a large bandwidth.

### Route 53

Amazon Route53 provides a high-availability and scalable DNS (Domain Name System) web service.

Advantages of Route53:

Extremely Reliable: AWS's highly available and dependable infrastructure is used in the construction of Route53. End users may be reliably routed to the web application thanks to the distributed architecture of the AWS DNS servers.

Scalable: It manages big queries without the user's help and automatically scales the resources during periods of high demand.

Secure: By integrating it with IAM, Amazon Route53's access is restricted to authorized users only, ensuring security.

Connected With Multiple AWS Services: It allows you to connect domain names to S3 buckets, Amazon EC2 instances, and other AWS resources.

### High Availability

The following are selected to achieve high availability for the AWS cloud services:

Multi-AZ Deployment: We deploy web tier, app tier and data tier applications across multiple Availability Zones to increase fault tolerance.

Elastic Load Balancing: This can distribute network traffic and workload across multiple instances in different subnets.

Auto Scaling group: It can automatically scale to adjust instance capacity to maintain performance.

### High Performance

The following are selected for high performance:

Three-tier architecture: To have web tier, app tier and data tier to separate user interface, application layer and data storage.

EC2 instance: To achieve managed, scalable and high-performance computing.

Amazon RDS/Aurora: To set up scalable, and high-performance databases.

## **Task 2A**

Explain in detail at least 4 advantages/disadvantages of moving software/hardware to a hybrid AWS cloud services and on-premises architecture? (Other cloud service provider is not accepted).

### Advantages of AWS

**User-friendly**

This tops the list of the Amazon Web Services benefits. Due to the platform's unique design for rapid and secure access, AWS is simple to utilize. Wherever and at any time, users are free to change their data. It is significantly simpler for most businesses to start using AWS as their cloud provider than alternative providers like Azure or Google Cloud Platform. AWS provides you with all the information, documentation, and video instructions to help you learn how to use all of its services.

**Flexible**

Another reason many businesses favour AWS is its flexibility. It always allows you to use the web application platforms, programming languages, and operating systems with which you are familiar. You can create your own virtual computing environment by installing your preferred operating systems and apps using a service like AWS EC2. The greatest services your application needs to run well are all included in AWS advantages. Additionally, it can facilitate the conversion process while allowing you to concurrently work on new solutions.

**Secure**

One of the greatest advantages of AWS cloud computing is security. As is well known, security is the top concern for any data-driven business. AWS offers an extremely secure infrastructure to protect your data privacy. AWS security experts adhere to several tiers of data monitoring, including:

* Data protection
* Identity and access management
* Infrastructure protection
* Threat detection and continuous monitoring
* Compliance and [data privacy](https://intellipaat.com/blog/what-is-data-privacy/)

It is an end-to-end strategy, allowing businesses to concentrate on company development rather than worrying about secrecy.

**Cost-effective**

If you use traditional methods, you must create your own servers to store your data and apps, which takes a significant amount of both time and money. So, instead of creating your own pricey servers, you can use AWS, where you just have to pay for the tools and services you need. AWS offers a pay-as-you-go pricing method, which means that a company will only pay for the services that it needs and has used for a period of time. It is the same as paying your electricity bill; you only pay for the units you have consumed. These [AWS services](https://intellipaat.com/blog/aws-services-list-and-products/) are unique and cheaper than the traditional computing method.

Moreover, AWS is a no-commitment service. It does not ask for any time commitment before you start using AWS benefits, so you can start or stop using it at any time without hassles.

### Disadvantages of AWS

**Limitations**

This comes first in the list of a few disadvantages of AWS Cloud Computing. AWS has some limits in terms of EC2 and security. Companies using AWS will have default resources to use, but the issue arises when default resource restrictions differ by location. Although they can request extra resources, businesses consider this a disadvantage of AWS.

**Lack of Experts**

AWS is the most recent invention with a sophisticated architecture. Companies that use Amazon Web Services as their cloud computing platform are looking for people to work on the cloud infrastructure. However, just a few professionals are knowledgeable about AWS or other cloud providers. Companies are eager to invest in them, but they are having problems hiring the proper experts to work on AWS who can drive their organizations to greater success. This can be a time and cost disadvantage for AWS.

**Price Variations**

AWS service prices vary by region, depending on the cost of land, Fiber, electricity, and taxes. Variations might occur when you require more technical support. Developer, Business, and Enterprise are the three available packages you can choose from, and the price varies accordingly. This will impact your monthly bill. But with services like [Amazon CloudWatch](https://intellipaat.com/blog/what-is-cloudwatch-in-aws/), you can monitor your service consumption, and Serverless Data Lake helps you calculate the cost of the services in your region.

**General Issues**

Amazon is a huge family with millions of customers, so it has some temporary [Cloud Computing](https://intellipaat.com/blog/what-is-cloud-computing/) issues. Users sometimes face downtime with servers. It may be because of the power loss or network connectivity with the cloud provider. Anyway, it can be rectified eventually.

Top Cloud Computing Platforms to Use [2025] - Intelli Paat

AWS service rates vary by region, based on the cost of land, Fiber, electricity, and taxes. Variations may arise when you seek more technical support.

## **Task 2B**

Identify 5 risks, analyze, and propose mitigating measures in detail clearly stating the security risks and how the security control & measures should be enabled and configured in moving some the operations to AWS cloud and some on-premises. All the identified potential vulnerabilities must be reference from the recent AWS threat landscape.

1. Compromised Access Credentials:

* **Risk:**

Unauthorized access to AWS resources due to stolen or leaked credentials, including IAM user credentials, root account credentials, and API keys.

* **Analysis:**

A compromised credential can grant an attacker full control over an AWS account, including the ability to modify resources, delete data, and create new resources.

* **Mitigating Measures:**
  + **Strong Authentication:** Implement Multi-Factor Authentication (MFA) for all IAM users and root accounts.
  + **Regular Rotation of Credentials:** Rotate API keys and other access credentials regularly and revoke them upon termination of an employee.
  + **Credential Monitoring:** Implement monitoring and alerting for suspicious activity related to credential usage.
  + **Least Privilege Access:** Grant users only the minimum necessary permissions required to perform their job duties.
  + **Secure Credential Storage:** Use AWS Secrets Manager or a similar solution for securely storing and managing sensitive credentials.

2. Misconfigured S3 Buckets:

* **Risk:**

Data breaches due to misconfigured S3 buckets that are publicly accessible or have overly permissive access controls.

* **Analysis:**

A misconfigured S3 bucket can allow anyone, including malicious actors, to upload, download, or delete data.

* **Mitigating Measures:**
  + **Bucket Configuration Validation:** Implement automated checks to ensure S3 buckets are configured correctly with the appropriate access controls.
  + **Object Versioning:** Enable object versioning to prevent accidental deletion of data.
  + **Secure Access Controls:** Configure S3 buckets with strong access controls, including IAM policies and bucket policies.
  + **Encryption:** Encrypt data at rest and in transit using S3 encryption.
  + **Logging and Monitoring:** Monitor S3 bucket activity for suspicious behaviour.

3. Excessive IAM Permissions:

* **Risk:**

Unauthorized access to AWS resources due to users or roles having excessive IAM permissions.

* **Analysis:**

Excessive IAM permissions can expose resources to unauthorized access and potentially allow attackers to escalate their privileges.

* **Mitigating Measures:**
  + **Principle of Least Privilege:** Grant users and roles only the minimum necessary permissions required to perform their job duties.
  + **IAM Role-Based Access Control:** Implement IAM roles to manage access to resources based on the role of the user.
  + **Regular Review of IAM Policies:** Regularly review IAM policies to ensure they are still appropriate and necessary.
  + **IAM Policy Simulation:** Use IAM policy simulation to test the impact of IAM policies on resource access.
  + **Access Control Lists (ACLs):** Use ACLs to further restrict access to resources.

4. Insecure APIs:

* **Risk:**

Exploitation of insecure APIs by attackers, leading to data breaches or other security incidents.

* **Analysis:**

APIs can be vulnerable to attacks such as injection attacks, cross-site scripting (XSS), and unauthorized access.

* **Mitigating Measures:**
  + **API Gateway:** Use AWS API Gateway to manage and secure APIs.
  + **API Security Controls:** Implement API security controls such as rate limiting, request validation, and access control lists.
  + **API Monitoring:** Monitor API traffic for suspicious behavior.
  + **API Security Testing:** Conduct regular API security testing to identify vulnerabilities.
  + **Secure Coding Practices:** Follow secure coding practices when developing APIs.

5. Insufficient Logging and Monitoring:

* **Risk:** Inability to detect and respond to security incidents due to insufficient logging and monitoring.

## **Task 2C**

Establish a roadmap to implement AWS cloud computing and on-premises set up in the organisation. What are the estimated costs (CAPEX and OPEX) of operation?

### Phase 1: Assessment and Planning (Weeks 1-4)

1. **Inventory existing infrastructure**: Document current on-premises infrastructure, including servers, storage, and network equipment.

**Current Network infrastructure**

(5-year lifespan, straight-line depreciation)

|  |  |  |
| --- | --- | --- |
| **Component** | **Quantity** | **Costs** |
| Leaf Switches | 4 | $48,000 |
| Spine Switches | 2 | $50,000 |
| Access Points | 100 | $120,000 |
| Wireless Controllers | 2 | $60,000 |
| Router | 2 | $30,000 |
| Firewall | 2 | $40,000 |
| Management Switch | 1 | $3,000 |
| Load Balancer | 2 | $18,000 |

**Current** **Server Infrastructure**

(5-year lifespan, straight-line depreciation)

|  |  |  |
| --- | --- | --- |
| **Component** | **Quantity** | **Costs** |
| Blade Chassis | 4 | $40,000 |
| Blade Servers | 32 | $256,000 |
| Fabric Interconnects | 4 | $100,000 |
| Rack Servers | 8 | $72,000 |

**Current** **Storage Infrastructure**

(5-year lifespan, straight-line depreciation)

|  |  |  |
| --- | --- | --- |
| **Component** | **Quantity** | **Costs** |
| SAN Switches | 4 | $60,000 |
| Storage Array | 2 | $80,000 |
| Backup Storage | 2 | $80,000 |

1. **Identify workloads for migration**: Determine which applications and workloads can be migrated to AWS, considering factors like security, compliance, and performance requirements.

**Components on premise**

|  |  |
| --- | --- |
| **Components** | **Reason** |
| UCS Servers | Host applications and services. |
| Storage | Local SAN/NAS for high-speed data access |
| Leaf & Spine Switches | High-speed, redundant switching fabric. |
| Firewalls | Secure traffic between internal and external networks. |
| Wireless APs | Provide Wi-Fi access to BYOD devices |
| Management Switch | For out-of-band device management |

**Components to migrate to AWS cloud.**

|  |  |  |
| --- | --- | --- |
| **AWS Service** | **Quantity** | **Est. Monthly Cost** |
| EC2 Instances | 50 | $3,500 |
| EBS Storage | 16TB | $2,500 |
| S3 Storage | 100TB | $2,300 |
| Direct Connect | 1 | $720 |
| Transit Gateway | 1 | $300 |
| VPN Connection | 1 | $37 |
| Data Transfer (Out) | - | $900 |
| CloudWatch | - | $200 |
| IAM, VPC, Route 53, etc. | - | $100 |

1. **Define security and compliance requirements**: Establish security policies, compliance requirements, and data governance frameworks for both on-premises and cloud environments.
2. **Develop a cloud strategy**: Outline operation aims, cost optimization strategies, and performance metrics for the hybrid cloud setup.

### Phase 2: AWS Setup and Migration (Weeks 5-12)

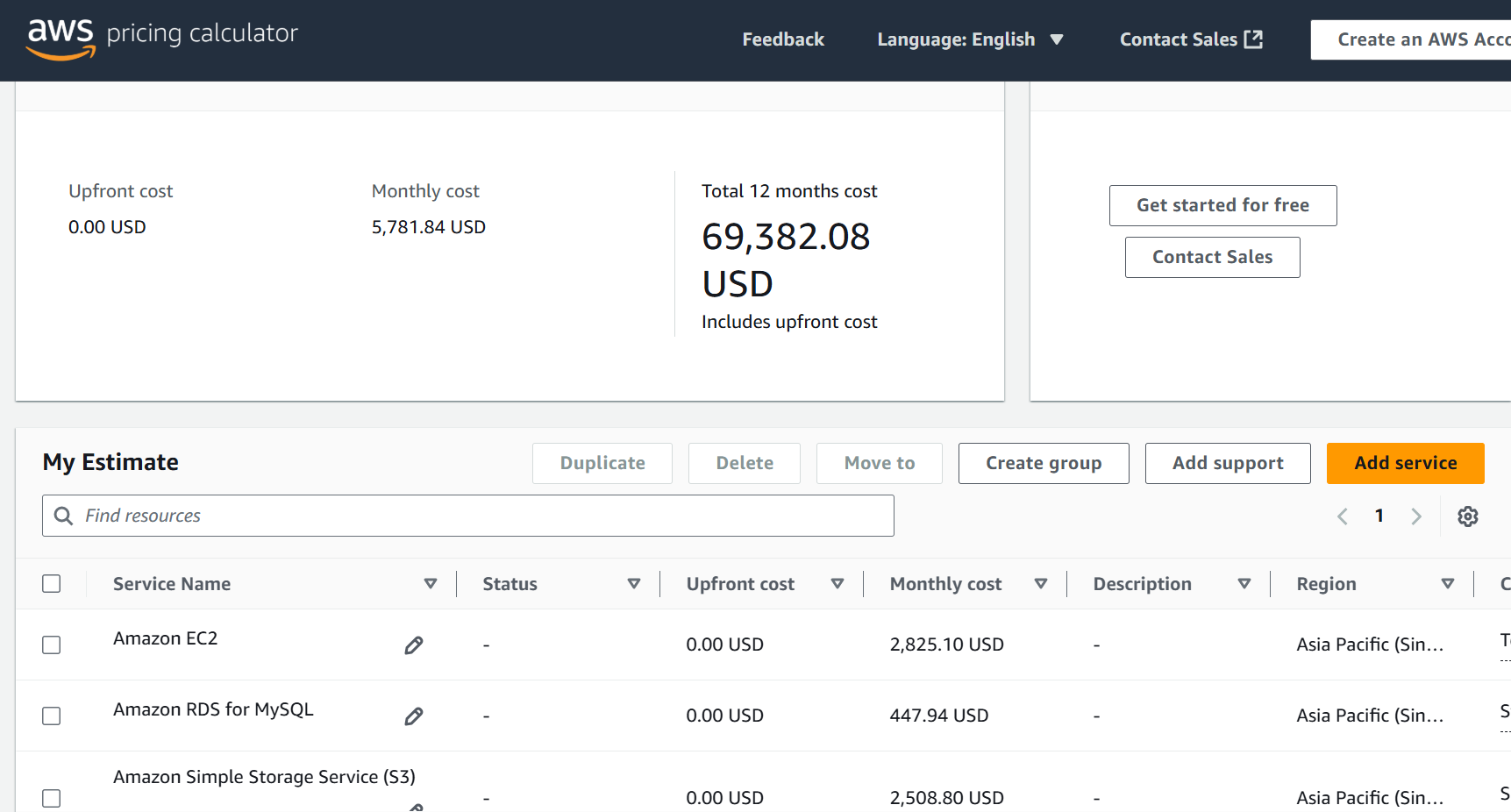
1. **Create an AWS account**: Set up an AWS account and configure the necessary IAM roles, users, and permissions.
2. **Provision AWS resources**: Create and configure AWS resources, such as EC2 instances, S3 buckets, and RDS databases, for migrated workloads.
3. **Migrate workloads**: Migrate identified workloads to AWS, using tools like AWS Migration Hub, AWS Database Migration Service, or third-party migration tools.
4. **Configure security and monitoring**: Set up security groups, monitoring tools (e.g., CloudWatch), and logging mechanisms for AWS resources.

### Phase 3: On-Premises Setup and Integration (Weeks 13-20)

1. **Upgrade on-premises infrastructure**: Upgrade or replace existing on-premises infrastructure to ensure compatibility with AWS services and meet business requirements.
2. **Configure hybrid connectivity**: Establish a secure and reliable connection between on-premises infrastructure and AWS using VPN, Direct Connect, or other connectivity options.
3. **Integrate on-premises and AWS services**: Integrate on-premises services with AWS services, such as using AWS Storage Gateway or AWS Outposts.
4. **Implement unified monitoring and management**: Set up unified monitoring and management tools to oversee both on-premises and AWS resources.

### Phase 4: Optimization and Maintenance (After Week 20)

1. **Monitor and optimize costs**: Use AWS Cost Explorer to track costs, identify optimization opportunities, and implement cost-saving measures.
2. **Continuously monitor performance**: Monitor performance metrics, identify bottlenecks, and optimize resources as needed.
3. **Maintain security and compliance**: Regularly review and update security policies, ensure compliance with regulatory requirements, and perform security audits.



### Estimated Costs (CAPEX and OPEX)

To estimate costs, let's consider:

* 50 EC2 instances (t2.large) running Windows
* 2 RDS instance (db.t2.medium) for database services
* 100 TB S3 storage for data storage
* 1 GB data transfer out per month

Total estimated monthly OPEX: $ 5781 USD

Total estimated yearly OPEX: $ 69,382 USD

CAPEX costs for on-premises infrastructure would depend on the specific hardware and software requirements. However, some estimated costs include:

* Network equipment: $335,000 USD (5-year lifespan, straight-line depreciation)

In summary, after migrating to cloud, for the next 5 years:

OPEX: $69K x 5 = $345 K USD

CAPEX: $335K USD

Total savings possible (5 yrs) = $343K USD

## **Conclusion**

In this report, we have proposed the possible plan to move the on-premises IT operations and infrastructure to the AWS cloud. We have provided the architecture diagram which aim to achieve high performance and high available for 4000 students computers with BYOD devices and 50+ servers currently in the polytechnic.

Furthermore, we have listed 4 advantages and disadvantages of moving to a hybrid AWS cloud services and on-premises architecture. And identified 5 risks, with analysis and propose mitigating measures against threats.

Finally, we have proposed a roadmap to implement the AWS cloud computing and on-premises setup for the polytechnic. The CAPEX and OPEX costs are included and total savings are shown.