

**Cloud Computing Security**

**Case Study - Proposal**

**Submission**

**SCHOOL OF INFORMATICS & IT**

**[Title of Assignment]**

Student Name (Matric Number) :

Tutorial Group :

Jenny LING (TP)

Tutor :

Submission Date :

**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.

Table of Contents

**Type chapter title (level 1)1**

Type chapter title (level 2)2

Type chapter title (level 3)3

**Type chapter title (level 1)4**

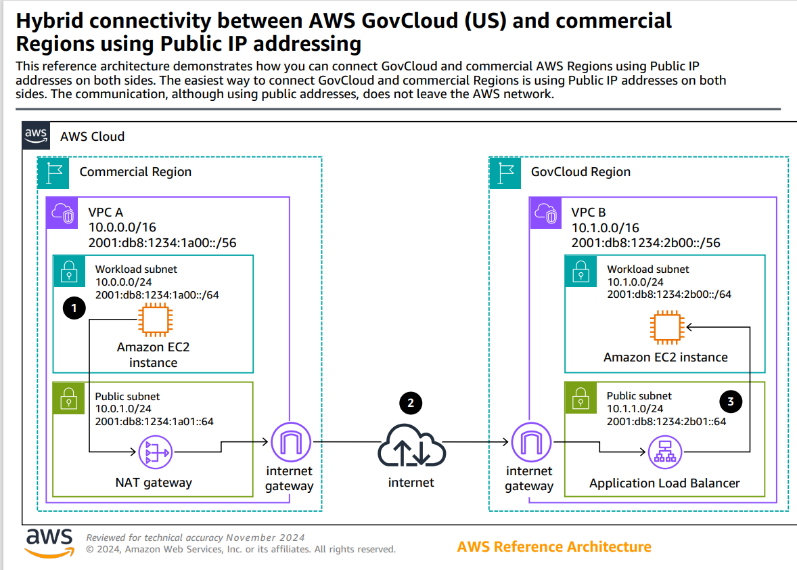
Type chapter title (level 2)5

Type chapter title (level 3)6

**Task 1**

Each group is required to propose and design ONE system and network architecture comprises of both AWS cloud and on-premises solution to achieve high performance and high availability as well as addressing migrating data from on-premises to cloud.

The proposed architecture is to be drawn and explained to justify the reason why such AWS and on-premises solution was selected. The architecture should also incorporate infrastructure for migration purposes such as having a transit gateway. The proposed architecture can be drawn in any design tools. All stated sub-tasks under task 2 must be linked to the architecture diagram.

****

Commercial Region:

AWS has many commercial regions globally, spanning across continents like North America, Europe, Asia, Australia, Africa, and South America. These regions are designed to accommodate diverse customer needs and preferences. AWS also has specific regions like AWS GovCloud (US) that are tailored for government entities and their unique compliance requirements.

1. Traffic outgoing an Amazon Elastic Compute Cloud (Amazon EC2) instance towards the Internet will follow the route table through the NAT gateway.
2. Traffic flows from the NAT gateway to the internet gateway of VPC A and into the Application Load Balancer (ALB) of VPC B in the GovCloud Region. This traffic does not leave the AWS global network.
3. Traffic flows from VPC B ALB to the target EC2 instance. Return traffic traverses the same path

GovCloud:

AWS GovCloud (US) is an innovative compliant cloud solution that technology leaders trust to host sensitive and controlled unclassified information (CUI) data, and is built to enable mission and business critical, high-value assets. It is comprised of two physically and logically isolated U.S. sovereign regions, AWS GovCloud (US-East and US-West), operated by U.S. citizens on U.S. soil that enable secure, scalable, and [resilient enterprise cloud architectures](https://pages.awscloud.com/govcloud-resiliency-imperatives-for-cios-with-sensitive-and-highly-available-cloud-environments.html). Connectivity is available from both the public Internet and privately with AWS Direct Connect.

What AWS services are in GovCloud?

* Application Auto Scaling.
* AWS AppConfig.
* AWS Application Migration Service.
* AWS Artifact.
* AWS Auto Scaling.
* AWS Backint Agent for SAP HANA.
* AWS Backup.
* AWS Batch.

**Task 2**

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).

**User-friendly**

This tops the list of the Amazon Web Services benefits. AWS is easy to use as the platform is specially designed for quick and secure access. Users can modify their data whenever they want, wherever they want. Most companies find starting with AWS as their cloud provider much easier than using other providers, namely, [Azure](https://intellipaat.com/blog/what-is-microsoft-azure/) or [Google Cloud Platform](https://intellipaat.com/blog/what-is-google-cloud/). AWS provides you with all the information, documentation, and video instructions to help you learn how to use all of its services.

**Flexible**

Flexibility is also the reason why many companies prefer AWS. It always lets you use those operating systems, programming languages, and web application platforms that you are comfortable with. With a service like AWS EC2, you can build your virtual computing environment by setting up your preferable operating systems and applications. AWS benefits provide all the best services that your application requires to function seamlessly. It can also ease the migration process, and you can work on new solutions simultaneously.

**Secure**

Security is one of the best benefits of AWS cloud computing. As we know, security is the uppermost priority for any company that is data-driven. AWS provides a highly secure infrastructure to ensure the privacy of your data. Security professionals at AWS follow different layers of data surveillance such as:

* 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 approach so that companies need not worry about their confidentiality, and instead, they can focus on business development.

**Cost-effective**

If you follow traditional methods, then you should build your own servers for storing your data and applications, which consumes a good amount of both your time and money. So instead of building your own expensive servers, you can use AWS where you need to pay only for the tools and services that you use. 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. In AWS, there are some limitations regarding EC2 and security. Companies that are using AWS will have default resources to use, but the problem comes when default resource limits vary from region to region. Although they can submit a request for more resources, companies find it a disadvantage of AWS.

**Lack of Experts**

AWS is the latest invention with a complex infrastructure. Companies using AWS as their [Cloud Computing platform](https://intellipaat.com/blog/cloud-computing-platforms/) are looking to hire professionals to work on the cloud infrastructure. However, only a few professionals are skilled in AWS or any cloud provider. Companies are ready to invest in them but are facing difficulty in finding the right professionals to work on AWS who can lead these organizations to better performance. This can be a disadvantage of AWS in terms of time and money.

**Price Variations**

The price of AWS services varies based on factors such as the cost of land, fiber, electricity, and taxes from region to region. Variations also occur when you need additional tech 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] - Intellipaat

Discover the top cloud computing platforms to use in 2025. AWS, Microsoft Azure, Google Cloud Platform, IBM Cloud, and Oracle Cloud are among the best options.

2b Identify 5 risks, analyse, 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 behavior.

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.

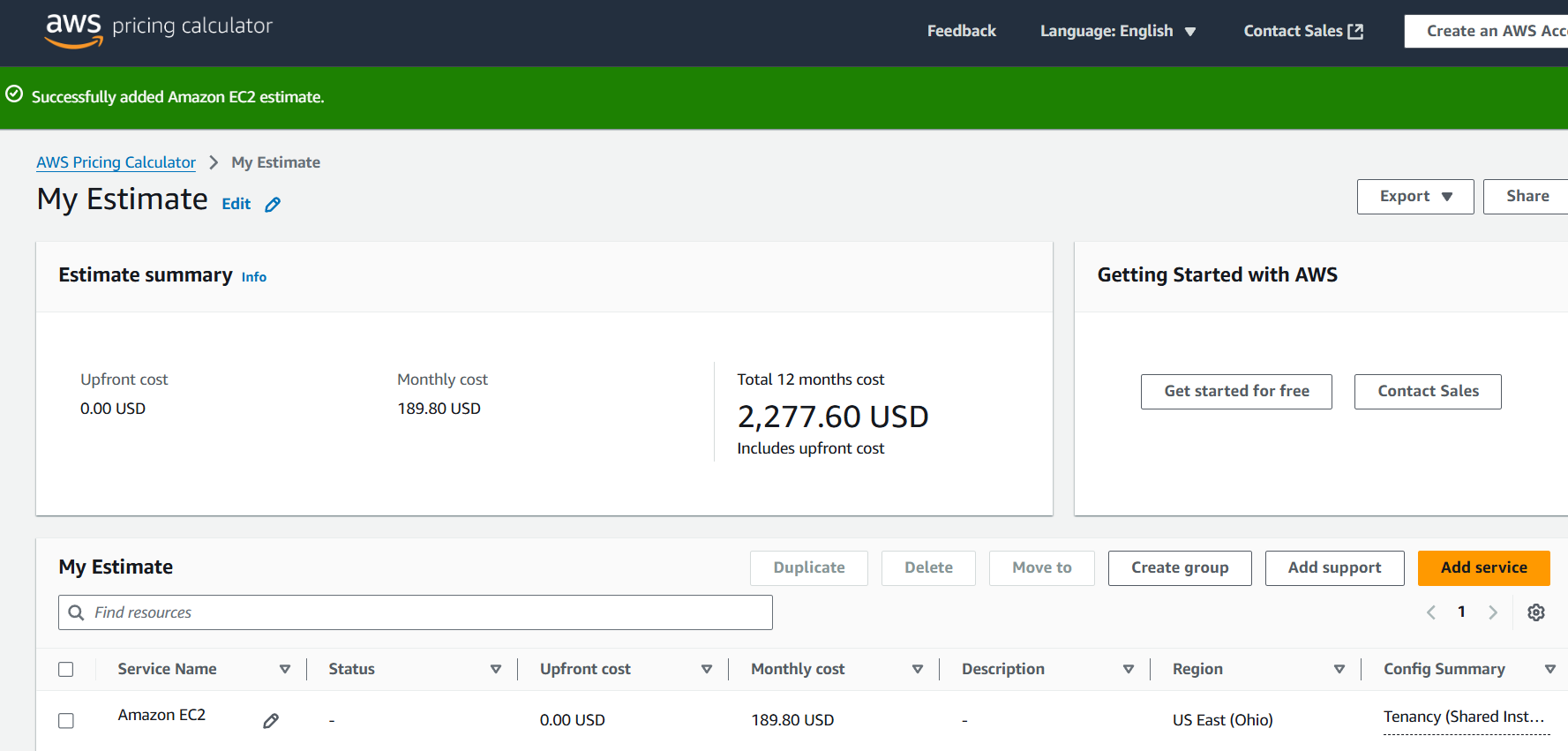
* **Mitigating Measures:**
  + **API Gateway:** Use AWS API Gateway to manage and secure APIs.
  + **API Security Controls:** Implement API security controls such as rate limiting, request validation, and access control lists.
  + **API Monitoring:** Monitor API traffic for suspicious behavior.
  + **API 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**

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? You are required to use AWS Cost Explorer

****

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

1. **Inventory existing infrastructure**: Document current on-premises infrastructure, including servers, storage, and network equipment.
2. **Identify workloads for migration**: Determine which applications and workloads can be migrated to AWS, considering factors like security, compliance, and performance requirements.
3. **Define security and compliance requirements**: Establish security policies, compliance requirements, and data governance frameworks for both on-premises and cloud environments.
4. **Develop a cloud strategy**: Outline business objectives, 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 a sample scenario:

* 10 EC2 instances (t2.medium) running Linux
* 1 RDS instance (db.t2.medium) for database services
* 100 GB S3 storage for data storage
* 1 GB data transfer out per month

Using AWS Cost Explorer, estimated monthly costs would be:

* EC2 instances: $189.80 ( Linux instances, t2.medium, 12 months)
* S3 storage: $0.26 (10 GB storage, 1 GB data transfer out)

Total estimated monthly OPEX: $1,182.39

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

* Server hardware: $50,000 (5-year lifespan, straight-line depreciation)
* Storage hardware: $10,000 (5-year lifespan, straight-line depreciation)
* Network equipment: $5,000 (5-year lifespan, straight-line depreciation)
* Software licenses: $10,000 (annual subscription fees)

To get a more accurate estimate, use AWS Cost Explorer to model your specific usage and costs. Consider factors like instance types, usage patterns, and data transfer requirements.

**AWS Cost Explorer**

AWS Cost Explorer is a powerful tool for estimating and managing AWS costs. To use it:

1. Log in to the AWS Management Console.
2. Navigate to the Cost Explorer dashboard.
3. Select the desired time range and granularity (e.g., monthly, daily).
4. Choose the services and resources to track (e.g., EC2, S3, RDS).
5. Analyze costs, identify trends, and optimize resources as needed.