**INTERNSHIP TASK -4**

**CLOUD SECURITY IMPLEMENTATION**

### **📌 Implementation Plan: IAM Policies, Secure Storage, and Data Encryption**

#### **1️⃣ IAM Policies (Identity & Access Management)**

✅ Implement **Least Privilege Access**:

* Create **custom IAM roles** with minimal permissions.
* Use **principle of least privilege (PoLP)** for users and service accounts.
* Example GCP IAM Policy (Restricting Cloud Storage Access):

sh

CopyEdit

gcloud projects add-iam-policy-binding [PROJECT\_ID] \  
--member=user:[USER\_EMAIL] --role=roles/storage.objectViewer

✅ Enable **Multi-Factor Authentication (MFA)** for admins.

#### **2️⃣ Secure Storage**

✅ Configure **Cloud Storage Access Controls**:

* Enforce **bucket-level IAM policies** to restrict unauthorized access.
* Enable **Cloud Audit Logging** to track storage activity.
* Example GCP Storage Policy (Restricting Public Access):

sh

CopyEdit

gsutil iam ch -d allUsers:objectViewer gs://[BUCKET\_NAME]

#### **3️⃣ Data Encryption**

✅ Enable **Encryption at Rest & In Transit**:

* Use **Cloud Key Management Service (KMS)** to manage encryption keys.
* Ensure data transmission over **TLS/SSL** (HTTPS endpoints).
* Example GCP KMS Key Creation:

sh

CopyEdit

gcloud kms keyrings create my-keyring --location global  
gcloud kms keys create my-key --location global --keyring my-keyring --purpose encryption

## **REPORT**

## **1. Introduction**

This report details the implementation of security best practices in a cloud environment, including **Identity and Access Management (IAM) policies**, **secure storage**, and **data encryption**. The goal is to enhance security by restricting unauthorized access, ensuring data integrity, and encrypting sensitive information both at rest and in transit.

## **2. IAM Policies Implementation**

### **2.1 Least Privilege Access Control**

* IAM roles were assigned based on the principle of least privilege.
* Custom roles were created to provide only necessary permissions for users and services.

### **2.2 Multi-Factor Authentication (MFA)**

* MFA was enforced for all administrators and privileged users.

### **2.3 Service Accounts and Role Binding**

* Dedicated service accounts were created for automated tasks.
* Example IAM policy binding in Google Cloud:

## **3. Secure Storage Implementation**

### **3.1 Storage Access Controls**

* Cloud Storage Buckets were configured with IAM policies to restrict access.
* Public access to sensitive storage buckets was removed.

### **3.2 Audit Logging**

* Cloud Audit Logs were enabled to track access and modifications to storage resources.

## **4. Data Encryption Implementation**

### **4.1 Encryption at Rest**

* Cloud Key Management Service (KMS) was used to encrypt stored data.
* Example of creating and using a KMS key in Google Cloud:

### **4.2 Encryption in Transit**

* Enforced TLS (SSL) encryption for all data transfers.
* HTTPS endpoints were configured for APIs and web applications.

## **5. Conclusion**

The implemented security measures effectively strengthen the cloud platform against unauthorized access and data breaches. IAM policies ensure proper access control, storage security measures prevent unauthorized data access, and encryption secures sensitive data both in transit and at rest.

## **6. Future Recommendations**

* Regular IAM policy reviews to ensure compliance with security best practices.
* Continuous monitoring of access logs for anomaly detection.
* Implementation of automated security audits and alerts.