**IMPLEMENT IAM POLICIES, SECURE STORAGE, AND DATA ENCRYPTION ON A CLOUD PLATFORM:**

**1.Implement IAM Policies (Identity and Access Management)**

**Instructions:**

* Use **IAM roles** to grant least privilege access.
* Define **custom roles** for more granular control.
* Use **service accounts** for applications instead of user credentials.
* Enable **organization policies** for security best practices.
* Implement **IAM conditions** to restrict access based on resource attributes.

### ****1.1 Define IAM Policies in GCP****

1. **Go to IAM in Google Cloud Console**
   * Open [**Google Cloud Console**](https://console.cloud.google.com/)
   * Navigate to **IAM & Admin > IAM**
2. **Assign Roles to Users/Service Accounts**
   * Click **Add**
   * Enter **Member (User/Service Account Email)**
   * Choose a **Role** (e.g., roles/storage.admin for Cloud Storage access)
   * Click **Save**
3. **Create Custom IAM Roles (If Needed)**
   * Go to **IAM & Admin > Roles**
   * Click **Create Role**
   * Define **permissions** and **assign users**
   * Save and apply the role
4. **Enable Multi-Factor Authentication (MFA)**
   * Go to **Security > Google Account**
   * Enable **2-step verification**
5. **Set Up Organization Policies (Optional)**
   * Go to **IAM & Admin > Organization Policies**
   * Apply **Security policies** (e.g., restrict public IPs, enforce encryption)

**IAM Policy Example (Using gcloud CLI)**

gcloud projects add-iam-policy-binding PROJECT\_ID \

--member="user:example@gmail.com" \

--role="roles/storage.admin"

**2. Secure Cloud Storage**

**Instructions :Google Cloud (GCP)**

* Use **Cloud Storage IAM policies** to control access.
* Enable **Bucket Lock** to prevent accidental deletions.
* Set up **VPC Service Controls** to prevent data exfiltration.
* Use **Cloud Storage Insights** to detect security risks.

### ****2.1 Create a Secure Cloud Storage Bucket****

1. **Go to Cloud Storage**
   * Open [**Google Cloud Storage**](https://console.cloud.google.com/storage/)
   * Click **Create Bucket**
2. **Set Access Control**
   * Choose **Fine-Grained** for **IAM-based access**
   * **Disable Public Access** to prevent unauthorized exposure
3. **Enable Bucket Lock (Optional, for Data Retention)**
   * Go to **Bucket Settings > Retention Policy**
   * Set a **retention period** to prevent deletion
4. **Use VPC Service Controls (To Prevent Data Exfiltration)**
   * Open [**VPC Service Controls**](https://console.cloud.google.com/security/service-perimeters)
   * Click **Create Perimeter**
   * Select **Cloud Storage as a protected resource**

**Bucket Access Example (Using gcloud CLI)**

gcloud storage buckets create my-secure-bucket \

--location=us-central1 \

--uniform-bucket-level-access

**3. Implement Data Encryption**

**Google Cloud (GCP)**

* **At-Rest Encryption:** Enabled by default using **Google-managed keys**.
* **Customer-Managed Encryption Keys (CMEK):** Use **Cloud KMS** for custom keys.
* **Client-Side Encryption:** Encrypt before uploading.
* **TLS (HTTPS) for Data in Transit**: Use **SSL/TLS** for secure connections.

### ****3.1 Enable Encryption for Cloud Storage****

1. **Go to Cloud Storage**
   * Click on **Bucket > Edit**
   * Select **Encryption Type: Customer-Managed Key (CMEK)**
2. **Create a Key in Cloud KMS**
   * Open [**Cloud KMS**](https://console.cloud.google.com/security/kms/keys)
   * Click **Create Key Ring > Create Key**
   * Choose **Key Purpose: Symmetric Encryption**
   * Enable **Rotation Policy** (Recommended every 90 days)
3. **Assign the KMS Key to Cloud Storage**
   * Open **Cloud Storage > Your Bucket > Edit**
   * Select **Use a customer-managed encryption key (CMEK)**
   * Choose the key from **Cloud KMS**
4. **Enable Encryption for BigQuery, Compute Engine, and Other Services**
   * For **BigQuery**: Enable **CMEK** under dataset settings
   * For **Compute Engine**: Use **CMEK while creating a disk**

**Encrypt Bucket with CMEK (Using gcloud CLI)**

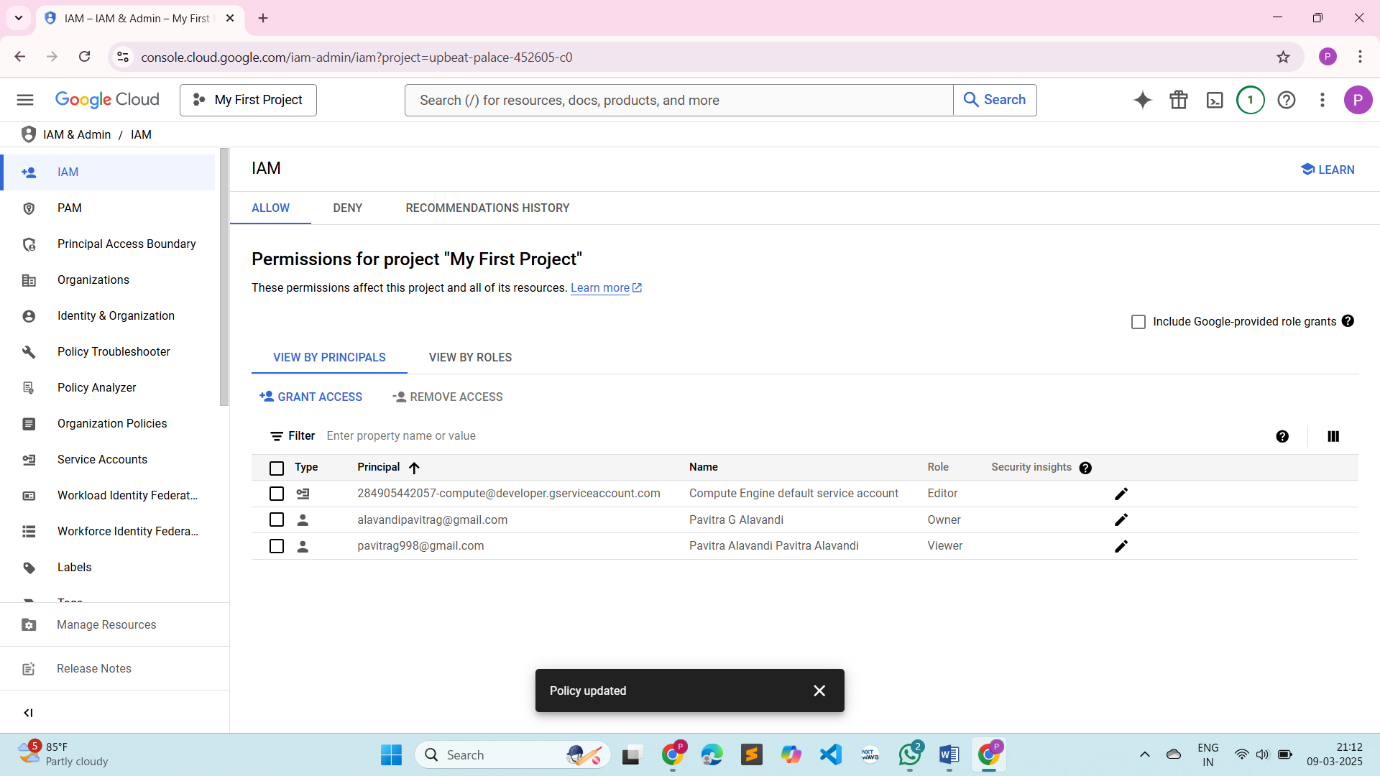
gcloud storage buckets update my-secure-bucket \

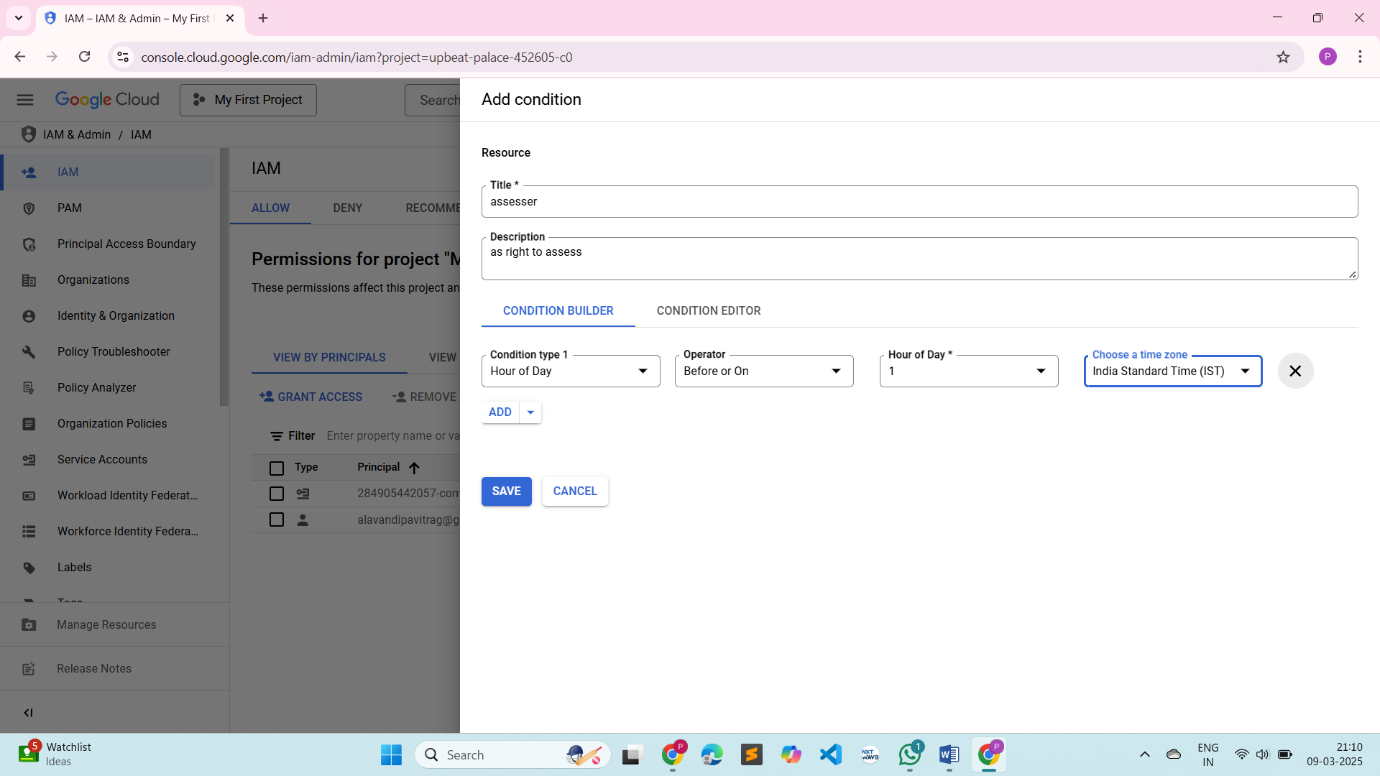
--encryption-key=projects/PROJECT\_ID/locations/global/keyRings/my-key-ring/cryptoKeys/my-key

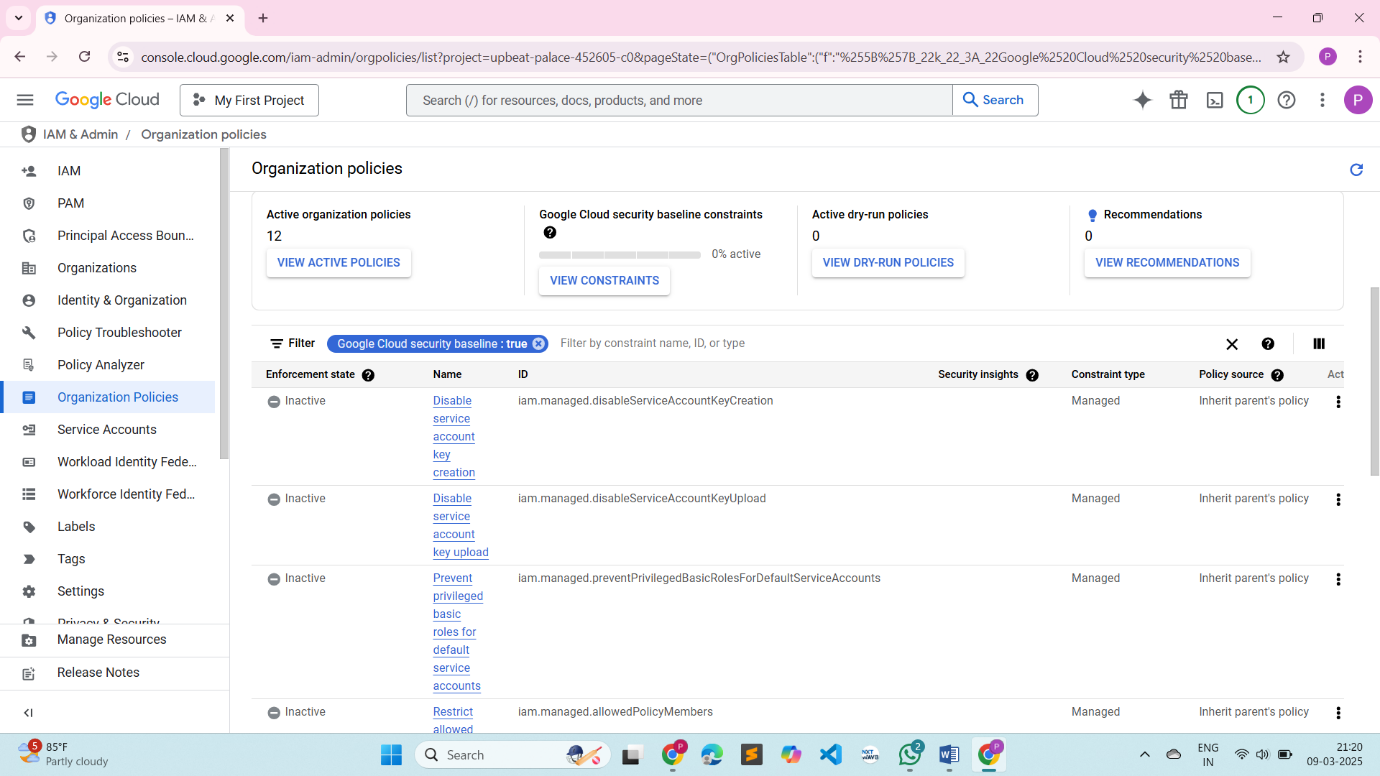
**Final Deliverable: Report Structure**

1. **Introduction**: Explain the purpose of securing .
2. **IAM Configuration**: Include Screenshots 1-3.
3. **Security**: Include Screenshots 4.
4. **KMS Encryption**: Include Screenshots 5.
5. **Conclusion**: Summarize how IAM, S3, and KMS enhance security.

IAM CONFIGURATIONS Screenshots:







Security

