Section 3

Design 2

Azure

6 Confluent Cloud is a SaaS for Apache Kafka. This service is chosen over self-hosted Kafka implementations for the easier architecture management and maintenance.

7 This design assumes the resources are within a Virtual Network with an NSG rule which allows outbound TCP connection to Confluent Cloud.

CONFLUENT

Confluent Cloud

1 API calls to Web Application 1 will go through the App Gateway. The App Gateway will enforce the HTTPS connection, redirecting the user to use the HTTPS connection if they are not on it. Otherwise, the App Gateway will act as the reverse proxy and forward the request to Web Application 1 for processing the image uploaded by the user.

2 The Web Application Firewall should also be configured on the App Gateway and be on **Prevention** mode to detect and block any anomaly and malicious requests after they meet the recommended threshold.

User
(PC or Mobile)

App Gateway + WAF

3 Web Application requires the User to be authenticated through AAD using the Organisation's Tenant Directory. The App Service hosting the Web Application 1 can be configured to managed this authentication process automatically.

Azure Active Directory
(Organisation's Tenant)

8 Kafka Streams App can be assigned with a Managed Identity resource which is configured with **Storage Blob Data Contributor** and **Key Vault Reader**.

9 The credentials/secrets to establish the connection to Confluent Cloud can be retrieved from Key Vault. Engineers can manage the secrets without downtime.

10 The App Service hosting the Kafka Streams App will be configured to **Scale Out** based on the CPU utilisation rate over a defined period of time. This can help alleviate pressure on the resources as the organisation grows.

Key Vault

Managed Identity
(Storage Blob Data Contributor + Key Vault Reader)

Kafka Streams App

App Service

Web Application 1

App Service

Managed Identity
(Storage Blob Data Contributor Role)

4 The App Service hosting the Web Application 1 will be configured to **Scale Out** based on the average number incoming requests over the number of instances of the Web Application 1 over a define period of time. This Autoscaling configuration can alleviate pressure on the resource if the organisation expanded.

5 Web Application 1 App Service can be assigned with a Managed Identity resource. The Managed Identity can configured with the **Storage Blob Data Contributor Role** which allows Web Application 1 to add images to the storage account container. Managed Identities do not require secrets management.

11 With Lifecycle Management for Storage Account, a Rule can be created against all Base Blobs (images) stored in the containers, which will delete the Base Blob after the 7th day since creation. This will align with the privacy and compliance requirements. Azure Storage Service Encryption (SSE) can automatically encrypt data before it is stored, and it automatically decrypts the data when retrieving it.

Image Container

Storage Account

Processing Script

Azure Functions

12 Image processing script deployed to Azure Functions will react to file uploads or changes in blob storage. Processed images are stored in blob storage and corresponding metadata is stored in Cosmos DB. Can be scaled to meet demand.

Azure Functions Sink Connector for Confluent Platform configured with SSL is used to ingest real-time incoming images and metadata.

13 Processed image metadata is stored in NoSQL database for analysis. Data is configured with 7 days TTL to purge expired data completely after retention period.
Encryption at rest is implemented by secure key storage systems, encrypted networks, and cryptographic APIs.

Metadata Store

Azure Cosmos DB

14 Power BI is the Business Intelligence tool of choice as it can integrate with data sources from Azure resources including Azure Cosmos DB and Blob storage.

15 **Shared Access Signatures** (SAS) can be generate from Storage Account Containers and they can be configured to be read-only, suitable for analytical purposes. Power BI can connect to the blob storage container using the generated SAS.

Power BI on Azure

Legend

- AAD – Azure Active Directory
- SaaS – Software as a Service
- Apache Kafka for Confluent Cloud is an Azure Marketplace offering that provides Apache Kafka as a service that is readily integrated with Azure Cloud.
- NSG – Network Security Groups
- TTL – Time to live (Defines retention period of data)
- SSL – Secure Socket Layer (Provides secure network communication)
- SAS – Shared Access Signatures (Provides secured delegated access to resources)