# Lab 1: Implementing Data Encryption and Protection

## Objectives

By the end of this lab, you will be able to:

1. Enable and configure encryption for data at rest in Azure Blob Storage.
2. Create and use Azure Key Vault to manage cryptographic keys and secrets.
3. Apply data masking techniques to protect sensitive information in datasets.

## Sections

1. Create an Azure Key Vault and a key and secret
2. Create a user-assigned identity and assign a role in Key Vault
3. Create a Storage Account with encryption enabled
4. Applying Data Masking Techniques

**Note:**

1. All the steps are to be done within VS Code and Azure Portal on your VM Machine.
2. There will be breakout rooms assigned for both individual and group labs.
3. Group ID: Every 4-5 participants will belong in a group and each group will have a Group ID [1-4]
4. Participant ID: Every participant will also get a unique number as participant id. This id along with group id will be used to help name Azure resources.

*Please remember and note your [Participant ID+Group ID]*

5. Once you are logged into your VM Machine. Login into Azure Portal
   a. Go to https://portal.azure.com
   b. Login with the supplied credentials (username and password).
      i. Each participant has a unique integer for their login [1-20] eg. vmuser[1-20]
      ii. For example, participant number 5 will have
         1. Username: vmuser5@acclod.ca
         2. Password: will be provided during the class.
   c. You will then see the landing Azure homepage. Dismiss any popups/message boxes

6. Although this is a group lab, every individual will complete the lab on their VM Machine. Individuals within a group are expected to discuss and help each other.

*It’s important that you enter all the resource names as the same as mentioned and only access the one that you have created as there will be many within a single group.*

## Section 1: Create an Azure Key Vault and a key and secret

### Steps

1. Login into Azure Portal
2. Type **"Key Vault"** on the search bar and select **"Key Vaults"** from the drop down. You will be redirected to **"Key Vaults"** page.
3. Click on **"+ Create"**
4. In the Create key vault page, fill in the following details:
    a. **Subscription**: Select subscription.
    b. **Resource group**: Select resource group.
    c. **Key vault name:** Enter a unique name, **aimlseckeyvault[participant id +group id]**(must be globally unique).

       For example: aimlseckeyvault216 (participant id as 21 and group id as 6)

    d. **Region:** Select your assigned Region.

       | Group1 | Group2 | Group3 | Group4 |
       |---|---|---|---|
       | East US 2 | West US | West US2 | Canada Central |

    e. **Pricing tier:** Standard.
    f. **Days to retain deleted vaults:** Enter "7"
    g. **Purge protection:** Select the "Enable purge protection"
    h. Leave all the other defaults and click on **"Next"**
5. **Access configuration** Tab
    a. **Permission Model: Select** Azure role-based access control.
    b. Accept all the other default and click on **"Review + Create"**
6. **Review+Create Tab**
    a. Let the validation run and pass.
    b. Click on **"Create"** and wait for the deployment to complete.
    c. Once the deployment is completed, click on **"Go to resource"**
7. **In the Key Vault blade, expand Objects and select Keys from the left-hand menu.**
    a. Click + Generate/Import.
    b. In the Create a key page:
        i. Options: Select Generate.
        ii. Name: Enter "storage-encryption-key[participant id+group id]."
        iii. Key type: RSA.
        iv. RSA key size: 2048.
    c. Click **"Create"**.
8. **In the Key Vault blade, expand Objects and select Secrets from the left-hand menu.**
    a. Click + Generate/Import.
    b. In the Create a secret page:
        i. Name: Any name you want to give
        ii. Secret value: Any value you want to give
    c. Click **"Create"**.
    d. Click on the secret name you have just created and click on the current version to see all the details.
    e. Click on **"Show Secret Value"** to see the value.

# Section 2: Create a user-assigned identity and assign a role in Key Vault

## Steps

1. Login into Azure Portal
2. Type **"Managed Identities"** on the search bar and select **"Managed Identities"** from the drop down. You will be redirected to **"Managed Identities"** page.
3. Click on **"+ Create"**
4. **Basics**
    a. **Subscription**: Select subscription.
    b. **Resource group**: Select resource group.
    c. **Region:** Select your assigned Region.

| Group1 | Group2 | Group3 | Group4 |
|---|---|---|---|
| East US 2 | West US | West US2 | Canada Central |

    d. **Name:** Enter a unique name, **useridentity[participant id +group id]**.
    For example: useridentity216 (participant id as 21 and group id as 6)
    e. Click on **"Review + Create"**
5. **Review+Create Tab**
    a. Let the validation run and pass.
    b. Click on **"Create"** and wait for the deployment to complete.
6. Go to the Key vault that you have created in previous section
7. Click on **"Access control"**
8. Click on **"+ ADD"** and **"Add role assignment"**
9. Add role assignment
    a. Under Job function roles, search **"Key Vault Crypto Service Encryption User"** and then select from the list and click on **"Next"**
    b. Assign access to **"Managed Identity"**
    c. Click on **"+ Select Members"**
10. Search the name of the user identity you have just created and select it.
11. Click on "**Select**" and click on "**Review + assign**" 2 times to assign it

# Section 3: Create a Storage Account with encryption enabled

## Steps

1. Login into Azure Portal
2. Type **"Storage Account"** on the search bar and select **"Storage Accounts"** from the drop down. You will be redirected to **"Storage Accounts"** page.
3. Click on **"+ Create"**
4. **Basics**
    a. **Subscription**: Select subscription.
    b. **Resource Group**: Select resource group.
    c. **Storage account name:** Enter a unique name, **aimlsecstorageaccount[participant id +group id]**(must be globally unique).
    For example: aimlsecstorageaccount216 (participant id as 21 and group id as 6)
    d. **Region:** Select your assigned Region.

| Group1 | Group2 | Group3 | Group4 |
|---|---|---|---|
| East US 2 | West US | West US2 | Canada Central |

    e. **Primary Service:** Azure Blob Storage or Azure Data Lake Storage Gen 2
    f. **Primary Workload:** Other
    g. **Performance:** Standard.
    h. **Redundancy:** LRS
    i. Click on **"Next"**
5. **Advanced** Tab
    a. Accept and review all the defaults and click on **"Next"**
6. **Networking** Tab
    a. Accept and review all the defaults and click on **"Next"**
7. **Data Protection** Tab
    a. Accept and review all the defaults and click on **"Next"**
8. **Encryption** Tab
    a. **Encryption type**: Select "Customer-managed keys"
    b. **Encryption key:** Select "Select a key vault and key"
    c. **Key store type**: select "Key vault"
    d. **Key vault:** "Select the key vault that you have created"
    e. Select the Key that you have previously created.
    f. **User-assigned identity**: Click on "Select an identity"
    g. Search for the user managed identity that you have created in the previous section. Select it and click on **"Add"**
    h. Click on **"Review + Create"**
9. **Review+Create Tab**
    a. Let the validation run and pass.
    b. Click on **"Create"** and wait for the deployment to complete.
    c. Once the deployment is completed, click on **"Go to resource"**
10. In the left-hand menu, under Data Storage, click **Containers**

a. Click **“+ Container”**
   i. Name: Enter **“secure-data”**
   ii. Click on **“Create”**

b. Click on the **“secure-data”** container that you just created.

c. Click **“Upload”**
   i. Browse to the **“sensitive-data.csv”** file and select that.

   ( You can download the file from SecureAzureAIMLWorkload/sensitive-data.csv at main · AshMinDI/SecureAzureAIMLWorkload · GitHub )

   ii. Click on **“Upload”**

d. Once file is uploaded, click on the file name and check if “**Server Encrypted”** is “**true**”

   This confirms that the data is encrypted at rest.

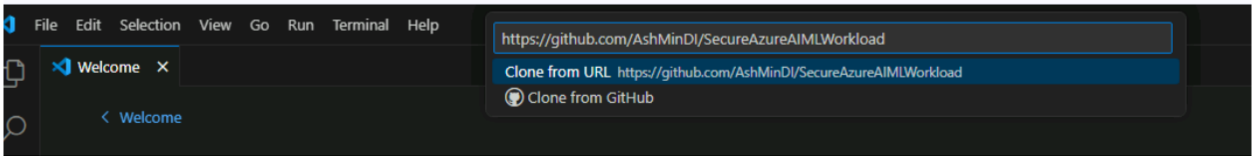
**11.** On the same screen, click on **“Generate SAS**” and click on “**Generate SAS token and URL**”

**12.** Copy the Blob SAS URL and save it to be used in next section.

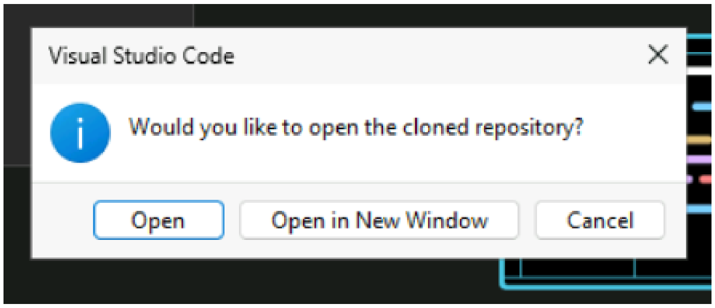
## Section 4: Applying Data Masking Techniques

### Steps

1. On your VM, open VS Code.
2. Enter “Ctrl+Shift+P” and type Git:Clone on the search window and press enter.
3. Paste https://github.com/AshMinDI/SecureAzureAIMLWorkload and press enter


File
Edit
Selection
View
Go
Run
Terminal
Help
Welcome ×
< Welcome
https://github.com/AshMinDI/SecureAzureAIMLWorkload
Clone from URL https://github.com/AshMinDI/SecureAzureAIMLWorkload
Clone from GitHub

4. In the browse window that opens, go to documents and **“Select as Repository Destination”**
5. Click on “**Open**” and click on “**Yes**, I trust the authors” if asked.

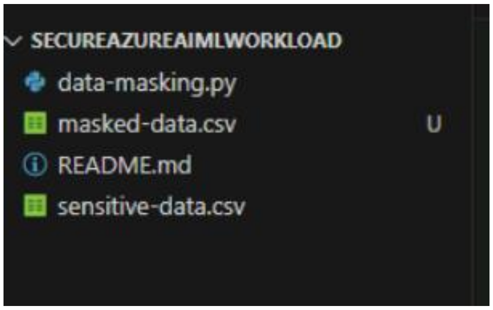


Would you like to open the cloned repository?

6. On the left side of the files, click on “**data-masking.py**” file. You will be prompted to install the python extension. Click on Install
7. Within **“data-masking.py”** change the line
   df = pd.read_csv('sensitve-data.csv’)
   to
   df = pd.read_csv('<SAS URL>’)

   and click on save.

8. Open Microsoft Store and wait for it to load. Type “**Python**” on the MS Store search bar and select **“Python 3.11”** and click on **“GET”.** Wait for Python to install. Once completed, close MS Store.
9. Once completed, On VS Code, click on Terminal menu on the top and click on **“New Terminal”.**
10. Type **“python --version”** on the VS Code terminal and now you should see the version
11. Type “pip install pandas” and let the package install. Ignore or close any warnings or environment creations.
12. Run “python data-masking.py” and it will create a new file called “masked-data.py”. Click on the file and you will see the fields in this file all masked.



*End of Lab.*