Participant Worksheet

Understanding cryptography implementation in cloud computing

Technical Description

This worksheet will help the participant to understand the application of computing cryptography in cloud computing environment.

Worksheet Output

1. Ability to secure the data by using client side encryption in the cloud.
2. Ability to design and to secure the data in the cloud
3. Ability to implement ready to use Office 365 protection

Tools and Software

1. Computer with sufficient specification for Windows 10.
2. Microsoft Visual Studio 2019
3. Microsoft Azure Subscription
4. Microsoft Office 365

Learning Activity

- □ Azure Client Side Encryption. - Demonstrates how to use encryption along with Azure Key Vault integration for the Azure Blob service.
    - Please visit https://azure.microsoft.com/en-us/resources/samples/storage-dotnet-client-side-encryption/
    - Please activate your azure free content at http://portal.azure.com
    - Activate your Azure Key Vault https://docs.microsoft.com/en-us/azure/key-vault/quick-create-cli
    - With Visual Studio follow the Section Running This sample by using visual studio or visual studio codes
    - Run the project
    - Learning activity 1 is finished
- □ Secure your cloud data.-Azure was designed for security and compliance. Learn how to leverage the built-in services to store your app data securely to ensure that only authorized services and clients have access to it.
    - Please visit https://docs.microsoft.com/en-us/learn/paths/secure-your-cloud-data/
    - First, design for security in Azure with Learn how to incorporate security into your architecture design, and discover the tools that Azure provides to help you create a secure environment through all the layers of your architecture.
    - Top five security items to consider before pushing to production. In learning how to secure your web applications on Azure and protect your apps against the most common and dangerous web application attacks.

- Secure your azure storage account. Learn how Azure Storage provides multilayered security to protect your data. Find out how to use access keys, to secure networks, and to use Advanced Threat Protection to proactively monitor your system.
- Manage secrets in your server apps with Azure Key Vault. Your application requires service passwords, connection strings, and other secret configuration values to do its job. Storing and handling secret values is risky, and every usage introduces the possibility of leakage. Azure Key Vault, in combination with managed identities for Azure resources, enables your Azure web app to access secret configuration values easily and securely without needing to store any secrets in your source control or configuration.
- Authenticate browser-based apps with Azure App Services. How to authenticate users using Azure App Services and various providers.
- Secure your Azure resources with conditional access. There's a tradeoff between security and ease-of-access. The conditional-access feature of Azure Active Directory helps you implement a good balance between the two. Learn how to implement a conditional-access policy using Azure Active Directory.
- Secure your Azure resources with role-based access control (RBAC). Learn how to use RBAC to manage access to resources in Azure.
- Secure your Azure SQL Database. Secure your Azure SQL Database to keep your data secure and diagnose potential security concerns as they happen.
- Learning secure your cloud data is finished.

- □ Successfully protect Office 365 and 3rd party cloud apps.- Microsoft Cloud App Security is Microsoft CASB (Cloud Access Security Broker) and is a critical component of the Microsoft Cloud Security stack. It's a comprehensive solution that can help your organization as you move to take full advantage of the promise of cloud applications, but keeps you in control through improved visibility into activity.
  - Configuring cloud apps Discovery. Discovery identifies current cloud apps, provides risk assessments and ongoing analytics and lifecycle management capabilities to control the use.
  - Active the conditional Access App Control with Office 365. utilizes a reverse proxy architecture and is uniquely integrated with Azure AD conditional access. Azure AD conditional access allows you to enforce access controls on your organization’s apps based on certain conditions.
  - Automate alerts management with Microsoft Flow. You can automate the triggering of playbooks when Cloud App Security generates alerts. For example, automatically create an issue in ticketing systems using ServiceNow connector or send an approval email to execute a custom governance action when an alert is triggered in Cloud App Security.
  - Improving Threat Protection Cloud App Security provides several threat detection policies using machine learning and user behavior analytics to detect suspicious activities across your different applications.
  - Activating Information Protection, Microsoft Cloud App Security helps you prevent this kind of disaster before it happens.