Secure – Data Security and Compliance Project

By: Karanam Sumanth
Email: sumanthkaranam2@gmail.com
College: Sree Vidyanikethan Engineering College, Information Technology

---

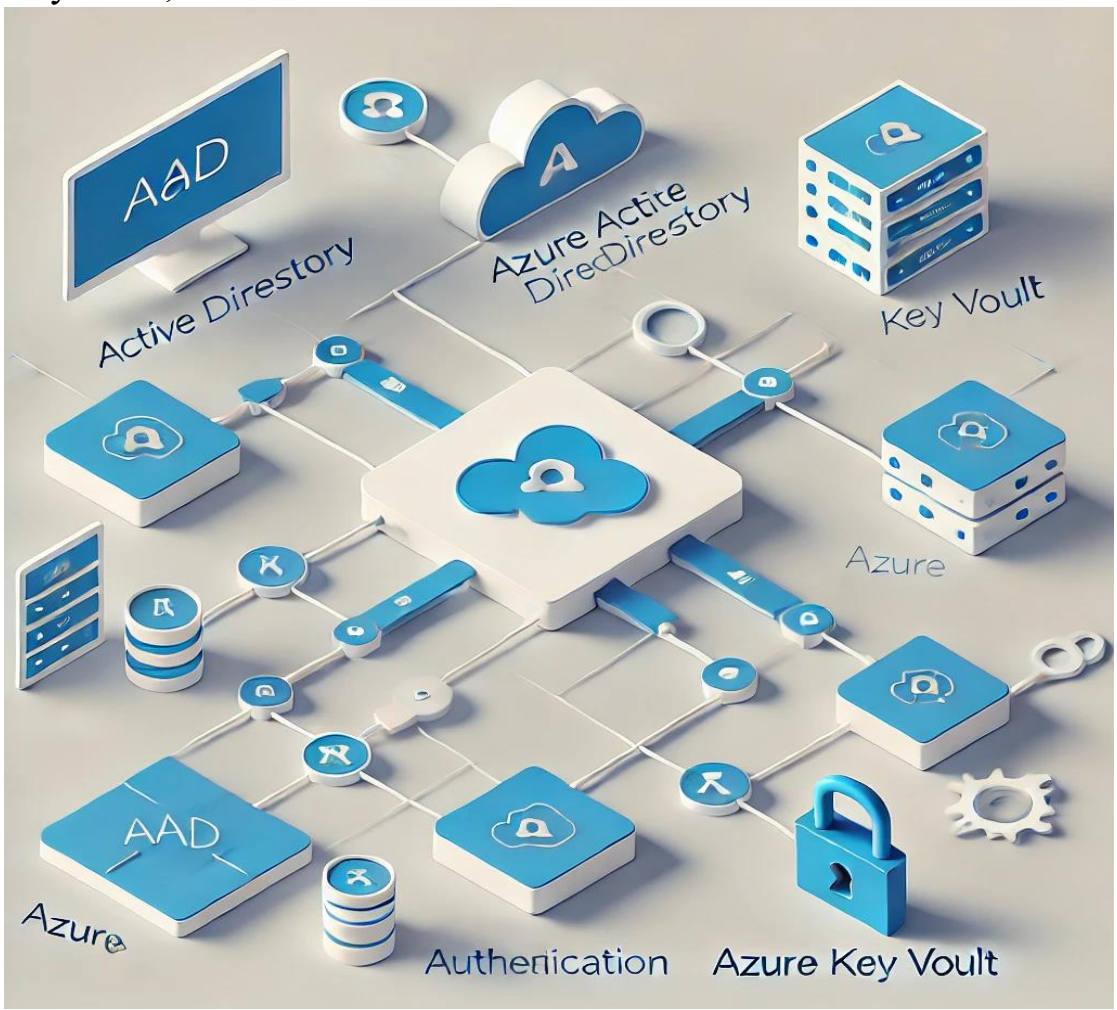
Overview

The project focuses on securing sensitive data and ensuring compliance using Microsoft Azure technologies. It leverages Azure Active Directory (AAD), Azure Key Vault, and Multi-Factor Authentication (MFA) for robust access control and data protection.

---

1. Architecture Diagram

The following diagram illustrates the interaction between AAD, Azure Key Vault, and MFA:



---

2. Configuration Details

A. Role-Based Access Control (RBAC)

Role	Description	Assigned To
Owner	Full control over resources.	IT Admin Group
Contributor	Manage resources but cannot assign roles.	Development Team
Reader	View resources without making changes.	Audit and Compliance

B. Access Policies for Azure Key Vault

Access Type	Permissions	Assigned To
Key Access	Get, List, Delete	IT Admin Group
Secret Management	Get, List, Update	Development Team
Certificate Access	Get, List	Security Team

C. Multi-Factor Authentication (MFA)

- **Policy Name:** Enforce MFA for Sensitive Resources
- **Scope:** Applies to all users accessing:
  - Azure Portal
  - Key Vault
- **Conditions:**
  - Require MFA for all sign-ins.
  - Apply MFA only for critical resource groups.

---

3. Implementation Steps

Step 1: Configure Azure Active Directory

- Add users and groups.

- Assign roles using **Access Control (IAM)**.

Step 2: Secure Sensitive Data with Azure Key Vault

- Store secrets like API keys and connection strings.
- Define access policies for roles and groups.

Step 3: Enforce Multi-Factor Authentication

- Create a Conditional Access policy in AAD.
- Enable MFA for all defined scopes.

Step 4: Monitor and Maintain Compliance

- Enable Microsoft Defender for Cloud.
- Generate compliance reports using Azure Compliance Manager.

---

4. Outcome

- **RBAC Implementation:** Defined granular access to Azure resources.
- **Data Security:** Secrets and keys are securely stored in Azure Key Vault.
- **Enhanced Authentication:** MFA ensures secure access to critical resources.
- **Compliance Monitoring:** Tools like Microsoft Defender and Compliance Manager provide continuous security assessments.