**ASSIGNMENT#4**

**Q) Briefly discuss how Microsoft Azure provides security?**

1. **General Azure security**

1. Azure Security Center

A cloud workload protection solution that provides security management and advanced threat protection across hybrid cloud workloads.

1. Azure Key Vault

A secure secrets store for the passwords, connection strings, and other information you need to keep your apps working.

1. Azure Monitor logs

A monitoring service that collects telemetry and other data, and provides a query language and analytics engine to deliver operational insights for your apps and resources. Can be used alone or with other services such as Security Center.

1. Azure Dev/Test Labs

A service that helps developers and testers quickly create environments in Azure while minimizing waste and controlling cost.

1. **Storage security**

1. Azure Storage Service Encryption

A security feature that automatically encrypts your data in Azure storage.

1. STORSIMPLE Encrypted Hybrid Storage

An integrated storage solution that manages storage tasks between on-premises devices and Azure cloud storage.

1. Azure Client-Side Encryption

A client-side encryption solution that encrypts data inside client applications before uploading to Azure Storage; also decrypts the data while downloading.

1. Azure Storage Shared Access Signatures

A shared access signature provides delegated access to resources in your storage account.

1. Azure Storage Account Keys

An access control method for Azure storage that is used for authentication when the storage account is accessed.

1. Azure File shares with SMB 3.0 Encryption

A network security technology that enables automatic network encryption for the Server Message Block (SMB) file sharing protocol.

1. Azure Storage Analytics

A logging and metrics-generating technology for data in your storage account.

1. **Database security**

1. Azure SQL Firewall

A network access control feature that protects against network-based attacks to database.

1. Azure SQL Cell Level Encryption

A database security technology that provides encryption at a granular level.

1. Azure SQL Connection Encryption

To provide security, SQL Database controls access with firewall rules limiting connectivity by IP address, authentication mechanisms requiring users to prove their identity, and authorization mechanisms limiting users to specific actions and data.

1. Azure SQL Always Encryption

Protects sensitive data, such as credit card numbers or national identification numbers (for example, U.S. social security numbers), stored in Azure SQL Database or SQL Server databases.

1. Azure SQL Transparent Data Encryption

A database security feature that encrypts the storage of an entire database.

1. Azure SQL Database Auditing

A database auditing feature that tracks database events and writes them to an audit log in your Azure storage account.

1. **Identity and access management**

1. Azure Role Based Access Control

An access control feature designed to allow users to access only the resources they are required to access based on their roles within the organization.

1. Azure Active Directory

A cloud-based authentication repository that supports a multi-tenant, cloud-based directory and multiple identity management services within Azure.

1. Azure Active Directory B2C

An identity management service that enables control over how customers sign-up, sign-in, and manage their profiles when using Azure-based applications.

1. Azure Active Directory Domain Services

A cloud-based and managed version of Active Directory Domain Services.

1. Azure Multi-Factor Authentication

A security provision that employs several different forms of authentication and verification before allowing access to secured information.

1. **Backup and disaster recovery**

1. Azure Backup

An Azure-based service used to back up and restore data in the Azure cloud.

1. Azure Site Recovery

An online service that replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location to enable recovery of services after a failure.

1. **Networking**
2. Network Security Groups

A network-based access control feature using a 5-tuple to make allow or deny decisions.

Azure VPN Gateway

1. A network device used as a VPN endpoint to allow cross-premises access to Azure Virtual Networks.
2. Azure Application Gateway

An advanced web application load balancer that can route based on URL and perform SSL-offloading.

1. Web application firewall (WAF)

A feature of Application Gateway that provides centralized protection of your web applications from common exploits and vulnerabilities

1. Azure Load Balancer

A TCP/UDP application network load balancer.

1. Azure ExpressRoute

A dedicated WAN link between on-premises networks and Azure Virtual Networks.

1. Azure Traffic Manager

A global DNS load balancer.

1. Azure Application Proxy

An authenticating front-end used to secure remote access for web applications hosted on-premises.

1. Azure Firewall

A managed, cloud-based network security service that protects your Azure Virtual Network resources.

1. Azure DDoS protection

Combined with application design best practices, provides defense against DDoS attacks.

1. Virtual Network service endpoints

Extends your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection.