ASSIGNMENT – 6

20BCSA09 – PRATYUSHA PRIYADARSHINI

1-Write down the key benefits of using RBAC provided by the MS Azure

ANS –

Fine-grained access control: Azure RBAC allows you to grant users and groups only the permissions they need to access Azure resources. This helps to reduce security risks by preventing unauthorized users from accessing sensitive data or making changes to critical systems.

Centralized management: Azure RBAC is a centralized authorization system, which means that you can manage access to all of your Azure resources from a single location. This makes it easier to keep track of who has access to what and to make changes to permissions as needed.

Scalability: Azure RBAC is designed to scale with your organization. As your organization grows, you can easily add new users and groups and assign them the appropriate permissions.

Reliability: Azure RBAC is a reliable authorization system that is backed by Microsoft's commitment to security and uptime. You can be confident that your Azure resources are protected from unauthorized access.

2- How do Azure Active Directory (AD) makes a difference in the the authentication system scenerio as compared to typical authentication process, explain it in your own words?

ANS-

Azure Active Directory (AD) is a cloud-based identity and access management (IAM) service that provides a single sign-on (SSO) experience for users to access applications and resources in the cloud and on-premises.

In a typical authentication process, users must provide a username and password to access an application or resource. This can be a time-consuming and frustrating process, especially if users have to remember multiple usernames and passwords for different applications and resources.

Azure AD simplifies the authentication process by allowing users to sign in with a single username and password across all applications and resources that are enabled for SSO. This makes it easier for users to access the applications and resources they need, and it reduces the risk of password-related security breaches.

In addition to SSO, Azure AD also provides a number of other features that can help to improve the security and manageability of your authentication environment, including:

Multi-factor authentication (MFA): MFA adds an additional layer of security by requiring users to provide a second form of identification, such as a code from their phone, in addition to their username and password.

Conditional access policies: Conditional access policies allow you to control who can access your applications and resources, and under what conditions. This can help to protect your resources from unauthorized access.

Self-service password reset (SSPR): SSPR allows users to reset their own passwords without having to contact the help desk. This can help to reduce the number of help desk tickets, and it can also improve the security of your environment by reducing the risk of users writing down their passwords.

Overall, Azure AD can help to improve the security, manageability, and user experience of your authentication environment. If you are looking for a cloud-based IAM solution, Azure AD is a great option.

Here are some additional ways that Azure AD can make a difference in the authentication system scenario:

Increased security: Azure AD provides a number of features that can help to improve the security of your authentication environment, such as MFA, conditional access policies, and SSPR.

Reduced costs: Azure AD can help to reduce costs by eliminating the need to manage and maintain your own on-premises identity infrastructure.

Improved compliance: Azure AD can help you to comply with industry regulations, such as HIPAA and PCI DSS.

Increased productivity: Azure AD can help to increase productivity by making it easier for users to access the applications and resources they need.