Seat No: _____ **Enrollment No: _____**

PARUL UNIVERSITY

FACULTY OF ENGINEERING & TECHNOLOGY

B.Tech. Summer/Winter 2023 - 24 Examination

Semester: **Date: (dd/mm/yyyy)**
Subject Code: (Subject Code) **Time: (2hr: 30min)**
Subject Name: (Subject Name) **Total Marks: 60**

Instructions:
1. All questions are compulsory.
2. Figures to the right indicate full marks.
3. Make suitable assumptions wherever necessary.
4. Start new question on new page.

Q.1	**Objective Type Questions** - (Fill in the blanks, one word answer, MCQ-not more than Five in case of MCQ) (All are compulsory) (Each of one mark)	**(15)**
	1. Which of the following is the identity authorization method A) Single Sign-on B) Multifactor Authentication C) Passwordless authentication D) All of Above Correct Answer : D) All of Above	
	2. Which method is used for connecting Azure Active Directory with your on-premises Active Directory A) B2B Direct Connect B) B2C Direct Connect C) Azure AD Connect D) Region Pairs Correct Answer : C) Azure AD Connect	
	3. Which Azure service allows you to host and manage web applications easily? A. Azure Functions B. Azure App Service C. Azure Kubernetes Service (AKS) D. Azure Logic Apps Correct answer: B) Azure App Service	
	4. Which Azure storage service is suitable for storing large binary objects like images or videos? A. Azure Blob Storage B. Azure Table Storage C. Azure File Storage D. Azure Queue Storage Correct answer: A. Azure Blob Storage	
	5. Which Azure pricing model allows you to pay only for the services you use, with no upfront commitment? A. Pay-as-you-go (PAYG) B. Reserved Instances C. Spot Pricing D. Consumption-based Pricing Correct answer: A. Pay-as-you-go (PAYG)	
	6. Azure Active Directory is used for identity and **access** management.	
	7. Encryption is a crucial component of "Defense in Depth" to protect **Data**	
	8. **Azure Virtual Network** allows you to create and manage virtual networks, including private and public IP addresses, subnets, and network security groups	

	9. DDoS stands for **Distributed** Denial of Service.	
	10. A region pair typically consists of **Two** regions.	
	11. How does Azure's pay-as-you-go pricing model work? Answer: Azure's pay-as-you-go pricing model allows users to pay only for the resources they consume. You are billed based on your actual usage of services, such as virtual machines, storage, and network bandwidth, on an hourly or per-minute basis.	
	12. Why is Azure App Service used for? Answer: Azure App Service is a platform-as-a-service (PaaS) offering that allows developers to build, host, and scale web applications and APIs without managing the underlying infrastructure.	
	13. Which Azure service allows you to deploy and manage virtual machines in the cloud? Answer: Azure Virtual Machines (VMs) enable you to deploy and manage virtualized Windows and Linux servers in the Azure cloud.	
	14. What is the purpose of Azure Blob Storage? Answer: Azure Blob Storage is used to store and manage unstructured data like documents, images, videos, and backups. It provides scalability, durability, and accessibility for data storage needs.	
	15. Which Azure service provides load balancing and traffic distribution across multiple virtual machines or services? Answer: Azure Load Balancer provides load balancing and traffic distribution across multiple virtual machines or services.	
Q.2	**Answer the following questions**. (Attempt any three)	**(15)**
	A) Name three Azure compute services and briefly explain their use cases. Answer (Any three based on Unit -2 Notes are Acceptable. Few examples are given below) **Azure Virtual Machines (VMs):** Use Case: Azure Virtual Machines provide scalable computing power for running a wide range of applications. Users can deploy virtual machines with various operating systems and customize them according to their specific needs. VMs are suitable for running traditional workloads, hosting applications, web servers, databases, and development and test environments. **Azure Functions:** Use Case: Azure Functions is a serverless compute service that allows you to run event-triggered code without provisioning or managing servers. It is ideal for executing short-lived, event-driven tasks or processes. Azure Functions are commonly used for event processing, data processing, automation, and building microservices in response to events from various Azure services or custom triggers. **Azure Kubernetes Service (AKS):** Use Case: Azure Kubernetes Service (AKS) is a fully managed Kubernetes service in Azure, offering a way to orchestrate and manage containerized applications at scale. AKS simplifies deploying, managing, and scaling containerized applications using Kubernetes. It is suitable for deploying microservices-based applications, enabling portability, scalability, and ease of management for containerized workloads. **Azure App Service:** Use Case: Azure App Service is a fully managed platform for building, deploying, and scaling web applications and APIs. It is an ideal choice for developers who want to focus on writing code without worrying about managing infrastructure. You can deploy web apps, mobile app backends, and RESTful APIs quickly and easily. Key Features: Support for multiple programming languages, automatic scaling, integration with Azure DevOps for continuous integration and deployment (CI/CD), and built-in security and monitoring tools.	

These Azure compute services offer flexibility and scalability, catering to different use cases and application requirements. Azure Virtual Machines provide the most control and customization, Azure Functions offer a serverless approach, and Azure Kubernetes Service facilitates efficient management of containerized applications.

B) Describe Azure role-based access control (RBAC)

Answer : Azure Role-Based Access Control (RBAC) is a comprehensive authorization system that allows administrators to control access to Azure resources, based on roles and permissions. It helps organizations manage permissions effectively by granting appropriate access to users, groups, and applications while restricting unauthorized access. RBAC is a fundamental part of Azure's security and governance framework, providing fine-grained control over who can do what within an Azure environment.

Key components and concepts of Azure RBAC include:

1. Roles:
   - Azure RBAC defines roles that encompass a set of permissions needed to perform a specific job or function within Azure. Roles can be Azure built-in roles (e.g., Owner, Contributor, Reader) or custom roles created by administrators.

2. Role Assignments:
   - Role assignments link users, groups, or applications to a specific role, granting them the associated permissions. An assignment can be made at various scopes, including management group, subscription, resource group, or individual resource.

3. Scope:
   - The scope defines the level at which a role assignment applies. It can be at the management group, subscription, resource group, or resource level. Permissions granted at a higher level in the hierarchy are inherited by lower levels.

4. Built-in Roles:
   - Azure provides a set of built-in roles, such as Owner, Contributor, Reader, and many more. These roles have pre-defined sets of permissions to simplify access management.

5. Custom Roles:
   - Administrators can create custom roles by defining specific permissions based on their requirements. Custom roles offer granular control over permissions, allowing precise access for users or applications.

6. Permissions:
   - Permissions are specific actions that a role can perform on an Azure resource or resource group. Each built-in or custom role is associated with a set of permissions.

7. Inheritance:
   - RBAC permissions are inherited based on the scope. If a user has a specific role assignment at a higher level, such as a subscription, they inherit those permissions for all resources under that subscription unless further restricted.

8. Azure AD Identities:
   - Users, groups, and applications from Azure Active Directory (Azure AD) are assigned roles in Azure. Azure AD is tightly integrated with Azure RBAC for user authentication and authorization.

	By implementing Azure RBAC, organizations can adhere to the principle of least privilege, ensuring that users have the minimum necessary permissions to perform their tasks. This helps enhance security, streamline access management, and maintain compliance with organizational policies and regulatory requirements.	
	C) What is Azure Blob Storage, and how is it typically used? Answer: Azure Blob Storage is a scalable and highly available cloud storage service provided by Microsoft Azure. It allows you to store and manage vast amounts of unstructured data in the cloud, such as text and binary data, including images, videos, documents, and application backups. Azure Blob Storage offers a durable, secure, and cost-effective solution for various storage needs. Azure Blob Storage is highly scalable, offers high availability, and provides a reliable and cost-effective solution for a wide range of storage needs, making it a vital component of many cloud applications and services.	
	D) Explain the concept of Azure B2B and B2C 1. Azure B2B (Business-to-Business): Answer: Azure B2B is a service that enables organizations to collaborate securely with external users, such as partners, vendors, or customers, while maintaining control and security over their own corporate resources. It allows businesses to extend their applications and services to external users without requiring them to have an organizational account in the Azure AD tenant. 2.Azure B2C (Business-to-Consumer): Azure B2C is a service designed to provide a secure and scalable identity management solution for consumer-facing applications. It is ideal for applications that need to authenticate a large number of users (consumers) using social identities (e.g., Facebook, Google) or local accounts.	

Q.3	**A) What is the Azure Pricing Calculator, and how can it assist in estimating costs?** Answer : The Azure Pricing Calculator is an online tool provided by Microsoft that helps users estimate the costs associated with using various Azure services. It allows you to calculate and understand the pricing details based on your specific requirements and usage patterns. How it can assist in estimating costs: Customized Configurations: Users can customize configurations based on their specific requirements, ensuring accurate cost estimates for their unique use cases. Cost Estimation for Architectural Planning: Architects and developers can use the calculator to estimate costs for designing new solutions, helping in budget planning and decision-making . Comparison of Scenarios: Users can compare different scenarios and configurations to understand how changes affect costs, allowing for cost optimization and efficient resource allocation. Budgeting and Forecasting:	**(07)**

	Organizations can use the calculator to forecast costs and plan budgets for upcoming projects, enabling better financial planning. Optimization and Decision Support: The Azure Pricing Calculator helps in optimizing costs by providing insights into potential savings through different configurations and usage patterns. Overall, the Azure Pricing Calculator is a valuable tool for users and organizations to estimate and plan their Azure spending, helping them make informed decisions, optimize costs, and stay within budget.	
	B) Define Azure Zero trust model Azure Zero Trust Model is a security framework and strategy that assumes no implicit trust for any user or system, regardless of their location (inside or outside the corporate network). In this model, every user, application, and device is treated as potentially untrusted, and access to resources is strictly controlled and verified through continuous authentication and authorization. Key principles and concepts of the Azure Zero Trust Model: 1. Verify Identity: - Implement strong multi-factor authentication (MFA) to verify the identity of users and devices before granting access to resources. 2. Least Privilege Access: - Grant the minimum level of access or permissions necessary for users, applications, and systems to perform their tasks. Regularly review and update access permissions based on roles and responsibilities. 3. Micro-Segmentation: - Implement network segmentation to isolate different parts of the network, limiting lateral movement and minimizing the potential impact of a security breach. 4. Continuous Monitoring: - Continuously monitor user and system behaviors, activities, and transactions to detect any suspicious or anomalous activities that may indicate a security threat. 5. Data Encryption: - Encrypt data at rest and in transit to ensure that sensitive information is protected, regardless of where it is accessed or stored. 6. Conditional Access: - Enforce access policies based on various conditions, such as user location, device compliance, time of day, and risk levels, to ensure secure access to resources. 7. Network Security: - Implement strong network security controls, such as firewalls, intrusion detection and prevention systems, and web application firewalls, to protect against external and internal threats. 8. Continuous Authentication and Authorization: - Use continuous authentication methods, such as behavioral analysis and risk-based access, to re-authenticate users and re-evaluate their access privileges during their session. 9. Workforce and Endpoint Security:	**(08)**

	- Ensure that endpoints are secure by implementing endpoint protection measures, including device encryption, anti-malware software, and regular security updates. 10. Policy Enforcement: - Enforce security policies consistently across all applications, regardless of whether they are hosted on-premises, in the cloud, or in hybrid environments. By adhering to the principles of the Azure Zero Trust Model, organizations can significantly enhance their security posture, reduce the risk of unauthorized access, and mitigate the impact of security breaches by minimizing the attack surface and enforcing strict access controls and continuous monitoring.	
	OR	
	C) What is a Virtual Machine (VM) in Azure? How does it differ from a physical machine, and what are its advantages? Answer: A Virtual Machine (VM) in Azure is a software-based emulation of a physical computer or server, created and hosted within the Azure cloud infrastructure. It allows users to run an operating system and applications as if they were on a dedicated physical machine, but in reality, they are running on shared hardware. Key characteristics of a Virtual Machine (VM) in Azure: 1. Software-Based Emulation: - VMs are created using virtualization technology, which allows multiple VMs to run on a single physical server, enabling efficient resource utilization and cost savings. 2. Isolation: - Each VM operates independently, with its own dedicated resources (CPU, memory, storage) and isolated environment, providing a level of security and stability. 3. Flexibility and Scalability: - VMs can be easily created, modified, and deleted to meet specific computing requirements. Azure provides various VM sizes, allowing scaling up or down based on demand. 4. Operating System Support: - VMs support a wide range of operating systems, including Windows Server, various distributions of Linux, and specialized OS versions, allowing compatibility with diverse workloads. 5. Hypervisor Technology: - VMs run on top of a hypervisor, a software layer that manages the sharing of physical resources and enables multiple VMs to run on a single physical machine. Differences from Physical Machines: 1. Hardware Independence: - VMs are not tied to specific hardware; they can be moved between physical servers without affecting their functionality, offering greater flexibility and portability compared to physical machines. 2. Resource Sharing: - VMs share physical hardware resources with other VMs on the same host, allowing efficient resource utilization and cost-effectiveness.	**(08)**

3. Ease of Provisioning:
- VMs can be rapidly provisioned and deployed, typically in a matter of minutes, compared to the time required to procure, set up, and configure physical hardware.

4. Resource Management:
- VMs can dynamically allocate or de-allocate resources like CPU and memory, enabling efficient usage of hardware and better cost management.

Advantages of Azure Virtual Machines:

1. Cost-Efficiency:
- VMs offer cost savings as they allow for efficient use of hardware resources by running multiple virtual machines on a single physical server.

2. Scalability:
- Azure VMs can easily scale vertically (resize to a larger VM) or horizontally (add more VMs) based on demand, providing flexibility and agility for changing workloads.

3. Isolation and Security:
- VMs provide isolation, enhancing security by separating workloads and applications, reducing the risk of one workload affecting another.

4. Disaster Recovery and Backup:
- Azure provides various tools and services to enable disaster recovery and backup strategies, ensuring high availability and data protection for VMs.

5. Flexibility and Compatibility:
- VMs support a wide range of operating systems and applications, making them suitable for diverse workloads and scenarios.

Overall, Azure Virtual Machines offer a highly flexible, efficient, and scalable solution for running various workloads in the cloud, allowing organizations to effectively manage their computing needs while optimizing costs.

Q.4	**A) Describe Service Lifecycles in Cloud Computing**	**(07)**

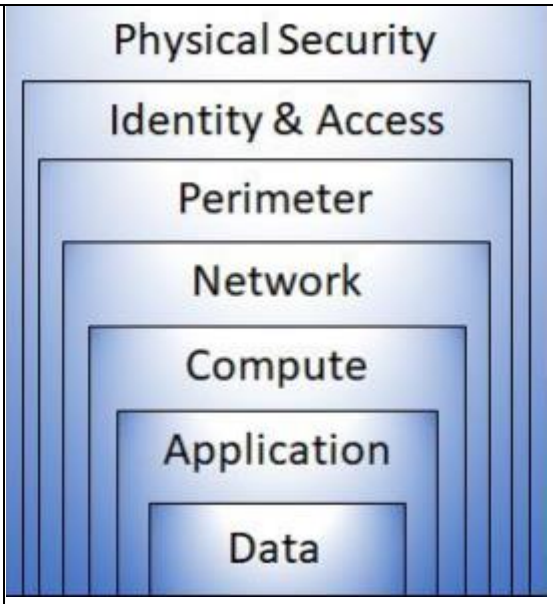
Answer:
The service lifecycle in cloud computing represents the various stages a cloud service or application goes through, from its inception and design to its eventual retirement. Managing the service lifecycle efficiently is crucial for ensuring the service's effectiveness, security, compliance, and cost-effectiveness. Here are the key stages in the service lifecycle in cloud computing:

1. Inception and Planning:
- In this stage, the idea for the service is conceived. The purpose, goals, scope, and initial requirements are defined. Planning involves assessing feasibility, potential benefits, and alignment with organizational objectives.

2. Design and Development:
- This stage involves detailed planning and designing of the service. Architects and developers create blueprints, define the architecture, select technologies, and start the development process based on the defined requirements.

3. Testing and Quality Assurance:

	- The service undergoes rigorous testing to identify and fix bugs, ensure functionality, security, performance, and compliance with specified requirements and standards. Quality assurance measures are implemented to meet high-quality standards. 4. Deployment and Provisioning: - The service is deployed to the cloud platform, and resources are provisioned accordingly. Configurations are set up, and the service becomes accessible to users or other applications. 5. Operations and Maintenance: - The service is actively used, and ongoing maintenance is performed to ensure its smooth operation. This includes monitoring, regular updates, patch management, scaling, and performance optimizations. 6. Monitoring and Management: - Continuous monitoring is essential to track service performance, user experience, security, compliance, and resource utilization. Management involves addressing issues, optimizing configurations, and making data-driven decisions. 7. Security and Compliance Management: - Security measures are continuously updated to address emerging threats and vulnerabilities. Compliance with industry standards and regulations is maintained through periodic audits and adjustments to security policies and configurations. 8. Optimization and Scaling: - As the service usage evolves, optimization and scaling measures are taken to improve efficiency, reduce costs, and ensure the service meets performance requirements even during peak usage. 9. Updates and Enhancements: - The service undergoes regular updates to add new features, improve performance, enhance security, and align with changing user needs and technological advancements. 10. End-of-Life Planning: - In this stage, plans are made for retiring the service. Data migration strategies, communication with users, and transition plans to alternative services are outlined. 11. Retirement and Decommissioning: - The service is retired and decommissioned. Data is securely disposed of, resources are deprovisioned, and users are transitioned to alternative services. Effectively managing each stage of the service lifecycle ensures that the cloud service remains efficient, secure, compliant, and aligned with organizational objectives throughout its existence.	
	OR	
	A) Briefly Explain The layers of defense-in-depth in azure Answer: The objective of defense-in-depth is to protect information and prevent it from being stolen by those who aren't authorized to access it. A defense-in-depth strategy uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data. Layers of defense-in-depth You can visualize defense-in-depth as a set of layers, with the data to be secured at the center and all the other layers functioning to protect that central data layer.	**(07)**



Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. This approach removes reliance on any single layer of protection. It slows down an attack and provides alert information that security teams can act upon, either automatically or manually.
Here's a brief overview of the role of each layer:

The physical security layer is the first line of defense to protect computing hardware in the datacenter.

The identity and access layer controls access to infrastructure and change control.

The perimeter layer uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.

The network layer limits communication between resources through segmentation and access controls.

The compute layer secures access to virtual machines.

The application layer helps ensure that applications are secure and free of security vulnerabilities.

The data layer controls access to business and customer data that you need to protect.

These layers provide a guideline for you to help make security configuration decisions in all of the layers of your applications.

Azure provides security tools and features at every level of the defense-in-depth concept. Let's take a closer look at each layer:

Physical security
Physically securing access to buildings and controlling access to computing hardware within the datacenter are the first line of defense.
With physical security, the intent is to provide physical safeguards against access to assets. These safeguards ensure that other layers can't be bypassed, and loss or theft is handled appropriately.
Microsoft uses various physical security mechanisms in its cloud datacenters.

Identity and access
The identity and access layer is all about ensuring that identities are secure, that access is granted only to what's needed, and that sign-in events and changes are logged.

At this layer, it's important to:

- Control access to infrastructure and change control.
- Use single sign-on (SSO) and multifactor authentication.
- Audit events and changes.

Perimeter

The network perimeter protects from network-based attacks against your resources.
Identifying these attacks, eliminating their impact, and alerting you when they happen are important ways to keep your network secure.
At this layer, it's important to:

- Use DDoS protection to filter large-scale attacks before they can affect the availability of a system for users.
- Use perimeter firewalls to identify and alert on malicious attacks against your network.

Network

At this layer, the focus is on limiting the network connectivity across all your resources to allow only what's required. By limiting this communication, you reduce the risk of an attack spreading to other systems in your network.
At this layer, it's important to:

- Limit communication between resources.
- Deny by default.
- Restrict inbound internet access and limit outbound access where appropriate.
- Implement secure connectivity to on-premises networks.

Compute

Malware, unpatched systems, and improperly secured systems open your environment to attacks. The focus in this layer is on making sure that your compute resources are secure and that you have the proper controls in place to minimize security issues.
At this layer, it's important to:

- Secure access to virtual machines.
- Implement endpoint protection on devices and keep systems patched and current.

Application

Integrating security into the application development lifecycle helps reduce the number of vulnerabilities introduced in code. Every development team should ensure that its applications are secure by default.
At this layer, it's important to:
• Ensure that applications are secure and free of vulnerabilities.
• Store sensitive application secrets in a secure storage medium.
• Make security a design requirement for all application development.

Data

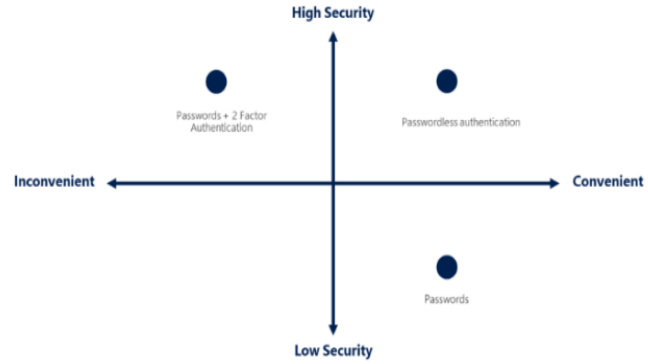
Those who store and control access to data are responsible for ensuring that it's properly secured. Often, regulatory requirements dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data.
In almost all cases, attackers are after data:
• Stored in a database.
• Stored on disk inside virtual machines.
• Stored in software as a service (SaaS) applications, such as Office 365.
• Managed through cloud storage.

B) Describe several azure Authentication methods in Detail **(08)**

Answer: Azure authentication methods
Authentication is the process of establishing the identity of a person, service, or device.
It requires the person, service, or device to provide some type of credential to prove who they are.
Authentication is like presenting ID when you're traveling. It doesn't confirm that you're ticketed, it just proves that you're who you say you are. Azure
supports multiple authentication methods, including standard passwords, single sign-on (SSO), multifactor authentication (MFA), and passwordless.

For the longest time, security and convenience seemed to be at odds with each other.
Thankfully, new authentication solutions provide both security and convenience.

The following diagram shows the security level compared to the convenience. Notice Passwordless authentication is high security and high convenience while passwords on their own are low security but high convenience.



single sign-on Single
sign-on (SSO) enables a user to sign in one time and use that credential to access multiple resources and applications from different providers. For SSO to work, the different applications and providers must trust the initial authenticator. More identities mean more passwords to remember and change. Password policies can vary among applications. As complexity requirements increase, it becomes increasingly difficult for users to remember them. The more passwords a user has to manage, the greater the risk of a credential-related security incident.

Consider the process of managing all those identities. More strain is placed on help desks as they deal with account lockouts and password reset requests. If a user leaves an organization, tracking down all those identities and ensuring they're disabled can be challenging. If an identity is overlooked, this might allow access when it should have been eliminated. With SSO, you need to remember only one ID and one password. Access across applications is granted to a single identity that's tied to the user, which simplifies the security model. As users change roles or leave an organization, access is tied to a single identity. This change greatly reduces the effort needed to change or disable accounts. Using SSO for accounts makes it easier for users to manage their identities and for IT to manage users.

Multifactor Authentication:

Multifactor authentication is the process of prompting a user for an extra form (or factor) of identification during the sign-in process. MFA helps protect against a password compromise in situations where the password was compromised but the second factor wasn't. Think about how you sign into websites, email, or online services. After entering your username and password, have you ever needed to enter a code that was sent to your phone? If so, you've used multifactor authentication to sign in.
Multifactor authentication provides additional security for your identities by requiring two or more elements to fully authenticate. These elements fall into three categories:

- Something the user knows – this might be a challenge question.
- Something the user has – this might be a code that's sent to the user's mobile phone.
- Something the user is – this is typically some sort of biometric property, such as a fingerprint or face scan.

Multifactor authentication increases identity security by limiting the impact of credential exposure (for example, stolen usernames and passwords). With multifactor authentication enabled, an attacker who has a user's password would also need to have possession of their phone or their fingerprint to fully authenticate.
Compare multifactor authentication with single-factor authentication. Under single-factor authentication, an attacker would need only a username and password to authenticate.
Multifactor authentication should be enabled wherever possible because it adds enormous benefits to security.

passwordless authentication
Features like MFA are a great way to secure your organization, but users often get frustrated with the additional security layer on top of having to remember their passwords. People are more likely to comply when it's easy and convenient to do so.
Passwordless authentication methods are more convenient because the password is removed and replaced with something you have, plus something you are, or something you know.
Passwordless authentication needs to be set up on a device before it can work. For example, your computer is something you have. Once it’s been registered or enrolled,
Azure now knows that it’s associated with you. Now that the computer is known, once you provide something you know or are (such as a PIN or fingerprint), you can be authenticated without using a password.
Each organization has different needs when it comes to authentication. Microsoft global Azure and Azure Government offer the following three passwordless authentication options that integrate with Azure Active Directory (Azure AD):

- Windows Hello for Business
- Microsoft Authenticator app
- FIDO2 security keys