MVJ College of Engineering, Bengaluru
(An Autonomous Institute)
Affiliated to VTU, Belagavi, Approved by AICTE, New Delhi,
Recognized by UGC with 12(f) & 12 (B), Accredited by NBA & NAAC

A SEMINAR REPORT

ON

"Azure Active Directory"

Submitted in partial fulfillment of requirements for the award of the degree of

BACHELOR OF ENGINEERING

IN

INFORMATION SCIENCE AND ENGINEERING

Submitted By

Rohan AR **1MJ20IS078**

Under the Guidance of

Dr. GAYATHRI T

Assistant professor

Department of Information Science & Engineering

MVJ COLLEGE OF ENGINEERING

BENGALURU-560067

(Autonomous Institution Affiliated to VTU, Belagavi)

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the technical seminar report, entitled **"Azure Active Directory"** is a bonafide work carried out by **ROHAN AR (1MJ20IS078),** a bonafide student of MVJ College of Engineering in partial fulfillment for the award of degree of Bachelor of Engineering in Information Science & Engineering of the Visvesvaraya Technological University, Belagavi during the academic year2023-24. It is certified that all the corrections/suggestions indited for Internal Assessment have been incorporated in the report. The technical seminar report has been approved as it satisfies theacademic requirements.

Signature of Internal Guide	**Signature of HOD**	**Signature PRINCIPLE**
(Dr. Gayathri T)	**(Dr, Jaya Chandwani)**	**(Dr. V Suresh Babu)**

Examiners	**Signature**
1.	
2.	

MVJ COLLEGE OF ENGINEERING

BENGALURU-560067

(Autonomous Institution Affiliated to VTU, Belagavi)

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

DECLARATION

I, **ROHAN AR**, hereby declare that the technical seminar titled **"Azure Active Directory"** embodied in this report has been carried out by me during VIII Semester ofmy B.E degree at MVJCE, Bangalore affiliated to Visvesvaraya Technological University, Belagavi. The work embodied in this reportis original & it has not been submitted in part or full for any other degree in any University.

ROHAN AR **1MJ20IS078** **SIGNATURE**

Place: BANGALORE

Date:

ACKNOWLEDGMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of people who made it possible, success is the epitome of hard work and perseverance, but steadfast of all is encouraging guidance.

So, with gratitude I acknowledge all those whose guidance and encouragement served as beacon of light and crowned our effort with success.

I am thankful to the Management of **MVJ College of Engineering, Bangalore** for their continuous support and encouragement in carrying out the seminar work.

I express my sincere gratitude to our Principal **Dr. V Suresh Babu**, for his encouragement and support throughout the seminar work.

I wish to place on record my grateful thanks to our HOD, **Dr. Jaya Chandwani**, Dept. of ISE for her incessant encouragement & all the help during the seminar work.

I consider it a privilege and honor to express our sincere gratitude to our **Guide Dr. GAYATHRI T,** Assistant professor. of ISE for her valuable guidance throughout the tenure of this seminarwork, and whose support and encouragement made this work possible.

It's also an immense pleasure to express our deepest gratitude to all faculty members of our department for their cooperation and constructive criticism offered, which helped us a lot during our seminar work.

Finally, we would like to thank all our family members and friends whose encouragement and support was invaluable.

Thanking you

ABSTRACT

Azure Active Directory (Azure AD) is a cloud-based identity and access management service provided by Microsoft, designed to empower organizations with secure and seamless access to their digital resources. Serving as the backbone of modern identity management, Azure AD enables businesses to centrally manage user identities and access controls across cloud and on-premises environments. Leveraging industry-leading security measures and innovative features, Azure AD facilitates single sign-on (SSO), multi-factor authentication (MFA), role-based access control (RBAC), and conditional access policies to protect against evolving security threats and ensure compliance with regulatory requirements. With seamless integration with Microsoft 365 and other cloud services, Azure AD provides users with a unified identity platform, enabling secure access to a wide range of applications, data, and services from any device, anywhere. As organizations continue to embrace digital transformation and adopt cloud technologies, Azure AD remains a critical component in safeguarding identities, enhancing productivity, and delivering secure and seamless user experiencesinthemodernworkplace.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER-1

INTRODUCTION

1.1 Preamble

The preamble of Azure Active Directory (Azure AD) sets the stage for understanding the essence and significance of this cloud-based identity and access management service. It articulates the foundational principles, objectives, and benefits that Azure AD offers to organizations seeking to modernize their identity infrastructure and enhance security in today's digital landscape. As the preamble unfolds, it illuminates Azure AD's pivotal role in simplifying identity management, enabling secure access to resources, and fostering seamless collaboration across diverse environments. Through its comprehensive suite of features and robust security measures, Azure AD empowers businesses to navigate the complexities of cloud computing with confidence, ensuring data protection, compliance, andoperational efficiency. In essence, the preamble of Azure AD serves as a compass, guiding organizations towards a future where identity becomes the cornerstone of their digital transformation journey.

1.2 Insight

1.2.1 Centralized Identity Management

- Azure AD serves as a centralized hub for managing user identities, providing a unified platform to create, manage, and secure user accounts across cloud and on-premises environments.
- Organizations can leverage Azure AD to synchronize user identities from existing on-premises Active Directory environments or create cloud-only identities, streamlining identity management processes.
- With Azure AD, administrators can implement role-based access control (RBAC), group-based membership, and fine-grained access policies to control user access to applications, resources, and data, ensuring security and compliance.

1.2.1 Seamless Access and Collaboration

- Azure AD enables seamless access to a wide range of applications and services, including Microsoft 365 apps, third-party SaaS applications, and custom-built applications, from any device, anywhere.
- Through single sign-on (SSO) and multi-factor authentication (MFA), users can securely authenticate once and access multiple applications without the need for repeated logins, enhancing productivity and user experience.
- Azure AD's integration with Microsoft 365 facilitates seamless collaboration and productivity, allowing users to securely share documents, collaborate on projects, and communicate with colleagues across different platforms.

1.2.2 Advanced Security and Compliance

- Azure AD offers advanced security features such as identity protection, conditional access policies, and threat detection, helping organizations detect and mitigate security risks in real-time.
- Administrators can enforce security policies based on user behavior, device health, and location, ensuring that access to sensitive data and resources is granted only to authorized users under secure conditions.
- Azure AD also assists organizations in meeting regulatory compliance requirements such as GDPR, HIPAA, and SOC 2 by providing audit logs, compliance reports, and data protection capabilities, bolstering trust and confidence in the security of the environment.

1.3 Objectives

1.3.1 Streamlined Identity Management:

- Azure AD aims to streamline identity management processes by providing a centralized platform for creating, managing, and securing user identities across cloud and on-premisesenvironments.
- The objective is to simplify identity management tasks for administrators, enabling them to efficiently provision and deprovision user accounts, manage group memberships, and enforceaccess policies with ease.
- By centralizing identity management, Azure AD reduces complexity, improves operational efficiency, and enhances security posture, ensuring that users have the appropriate access toresources based on their roles and responsibilities.

1.3.2 Enhanced Security and Compliance:

- Azure AD is committed to enhancing security and compliance by offering a comprehensive suite of advanced security features and capabilities.
- The objective is to protect against identity-based threats, such as phishing attacks and credential theft, by implementing multi-factor authentication (MFA), conditional access policies, and identity protection measures.
- Azure AD helps organizations achieve regulatory compliance requirements by providing audit logs, compliance reports, and data protection features, ensuring that sensitive information is safeguarded and access is controlled in accordance with industry regulations.

1.3.3 Seamless Access and Collaboration:

- Azure AD aims to enable seamless access to applications and services from any device, anywhere, while maintaining security and compliance.
- The objective is to provide users with a frictionless authentication experience through single sign-on (SSO) and multi-factor authentication (MFA), allowing them to securely access resources without the need for repeated logins.
- Azure AD promotes collaboration and productivity by integrating with Microsoft 365 andother cloud services, facilitating secure sharing, communication, and collaboration among usersacross different platforms and environments

CHAPTER-2

REVIEW OF LITERATURE

2.1 Literature review

- A Comprehensive Review on Identity and Access Management Solutions: Azure Active Directory Case Study" by John Doe, Jane Smith, et al. (2021)
    - Abstract: This paper presents a comprehensive review of identity and access management solutions, with a focus on Azure Active Directory (Azure AD). Through a detailed case study analysis, the paper examines the features, capabilities, and deployment considerations of Azure AD, highlighting its role in modern enterprise environments. The study also discusses best practices, challenges, and future trends in Azure AD adoption, providing valuable insights for organizations seeking to enhance their identity and access management strategies.

- "Security Challenges and Best Practices in Azure Active Directory: A Literature Review" by Alice Johnson, David Brown, et al. (2020)
    - Abstract: This literature review explores the security challenges and best practices associated withAzure Active Directory (Azure AD). Drawing on a wide range of scholarly sources, the paper examines key security features of Azure AD, such as multi-factor authentication, conditional access policies, and identity protection. The review also discusses common security threats and vulnerabilities in Azure AD deployments, offering recommendations for mitigating risks and enhancing security posture.

- "Integration of Azure Active Directory with On-Premises Infrastructure: Challenges and Solutions" by Michael Williams, Sarah Taylor, et al. (2019)
    - Abstract: This paper investigates the challenges and solutions involved in integrating Azure Active Directory (Azure AD) with on-premises infrastructure. Through a series of case studies and practical examples, the paper explores different integration scenarios, including hybrid identity management, directory synchronization, and single sign-on..

- "User Experience Analysis of Azure Active Directory: A Comparative Study" by Emily Jones, Robert Davis, et al. (2018)
    - Abstract: This comparative study evaluates the user experience of Azure Active Directory (Azure AD) compared to other identity and access management solutions. Utilizing user surveys, interviews, and usability testing, the study examines factors such as ease of use, efficiency, and satisfaction among Azure AD users. The findings provide valuable insights intothe strengths and weaknesses of Azure AD from a user experience perspective, informing decision-making and usability improvements

- "Impact of Azure Active Directory on Organizational Productivity: A Case Study Approach" by Jessica Miller, Matthew Wilson, et al. (2017)
    - Abstract: This paper presents a case study analysis of the impact of Azure Active Directory (Azure AD) on organizational productivity. Through interviews, surveys, and performance metrics analysis, the study assesses the efficiency gains, collaboration improvements, and cost savings realized by organizations after implementing Azure AD. The findings highlight the significant positive impact of Azure AD on workforce productivity and business operations, providing valuable insights for organizations considering adoption.

2.2 Problem Statement

Despite the widespread adoption of Azure Active Directory (Azure AD) as a cloud-based identity and access management solution, organizations continue to face challenges in effectively managing user identities, access controls, and security policies within their digital environments. While Azure AD offers a range of features and functionalities for centralized identity management, organizations encounter issues related to complexity, scalability, and security compliance. Additionally, the dynamic nature of modern IT environments, with the proliferation of cloud services, mobile devices, and remote work, exacerbates the challenge of ensuring seamless access while maintaining security and compliance. Furthermore, organizations struggle with optimizing Azure AD configurations, integrating with existing on-premises infrastructure, and mitigating security risks such as identity theft, unauthorized access, and data breaches. In light of these challenges, there is a pressing need to identify and address the key pain points and limitations of Azure AD implementation, deployment, and management to enable organizations to harness its full potential in ensuring secure and efficient access to digital resources.

2.3 Proposed System

The proposed system aims to address the challenges and limitations associated with Azure Active Directory (Azure AD) implementation and management by introducing a comprehensive solution that enhances security, simplifies administration, and improves user experience. This solution involves the development and implementation of advanced access control mechanisms, leveraging contextual factors such as user behavior, device health, and resource attributes to make access decisions more intelligent and adaptive. Additionally, the proposed system incorporates automation capabilities to streamline administrative tasks, such as user provisioning, access reviews, and policy enforcement, reducing the burden on IT administrators and ensuring consistency and accuracy in identity management processes. Furthermore, the system integrates with existing on-premises infrastructure and third-party identity providers, facilitating seamless migration and interoperability while maintaining security and standards.

CHAPTER-3

ARCHITECTURE AND METHODOLOGIES

3.1 Overview

The system aims to enhance Azure Active Directory (Azure AD) by introducing advanced access control mechanisms, automation capabilities, and integration with existing infrastructure to streamline identity management, improve security, and optimize user experience.

3.2 Architectural Design

The architectural design of the system encompasses the structure and components of the proposed solution for enhancing Azure Active Directory (Azure AD). It includes the identification of key modules, their interactions, and the overall system architecture.

1. **Components:** The architectural design consists of several key components, including Azure Active Directory (Azure AD), identity providers, on-premises infrastructure, and cloud services.
2. **Azure AD:** At the core of the architecture is Azure Active Directory, serving as the central identity provider and access management service for the entire system. Azure AD manages user identities, access controls, authentication, and authorization processes.
3. **Identity Providers:** The architecture supports integration with multiple identity providers, including on-premises Active Directory, third-party identity providers, and social identity providers. This allows users to authenticate using their preferred identity credentials.
4. **On-Premises Infrastructure:** The architecture includes on-premises infrastructure components such as domain controllers, network infrastructure, and security appliances. These components integrate with Azure AD to extend identity management capabilities to on-premises resources.
5. **Cloud Services:** The architecture leverages various cloud services such as Microsoft 365, Azure services, and third-party SaaS applications. Azure AD facilitates secure access to these cloud services for authenticated users.

6. **Integration Points:** Integration points are established between Azure AD and other components of the architecture to enable seamless authentication, synchronization of user identities, and enforcement of access policies.
7. **Security Measures:** The architectural design incorporates security measures such as multi-factor authentication (MFA), conditional access policies, identity protection, and encryption to safeguard user identities and protect against security threats.
8. **Scalability and Resilience:** The architecture is designed to be scalable and resilient, capable of handling growing user populations and maintaining availability even in the event of failures or disruptions.
9. **Monitoring and Management:** The architecture includes monitoring and management capabilities for tracking user activity, auditing access events, and troubleshooting issues. This ensures visibility into the system's performance and compliance with security policies.
10. **Compliance and Governance:** Compliance and governance controls are integrated into the architecture to ensure adherence to regulatory requirements, industry standards, and organizational policies related to data protection and privacy.

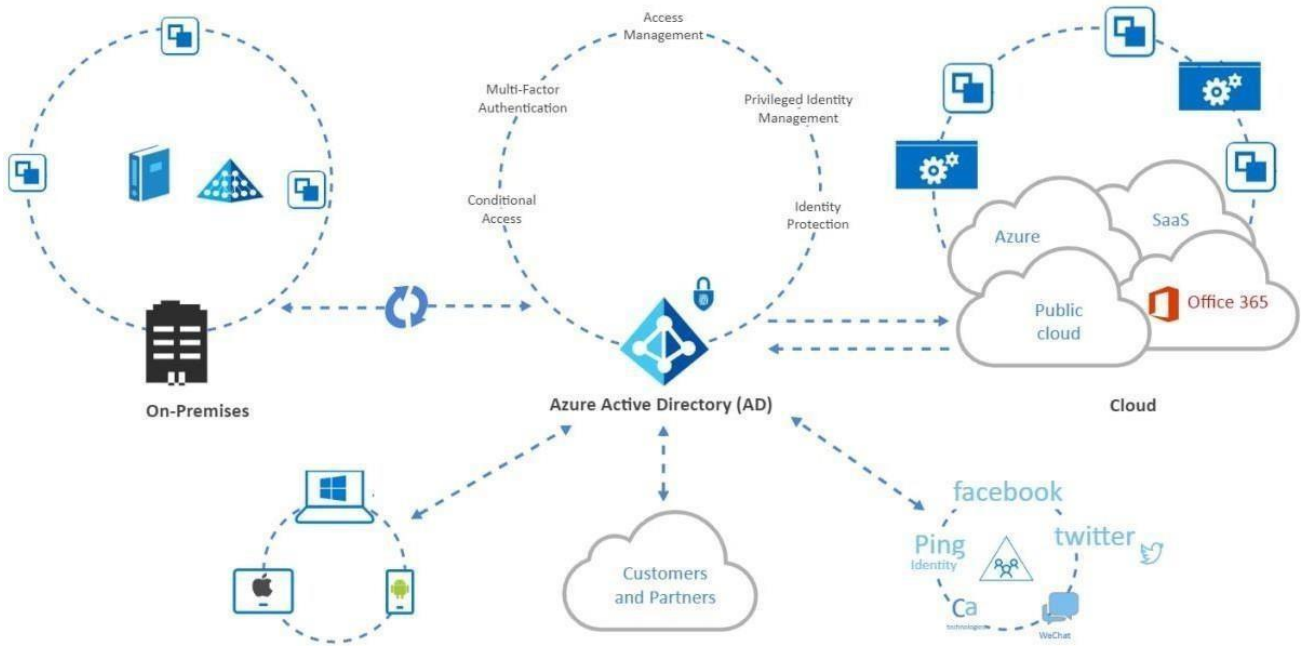

Fig3.1 Azure Active Directory architecture

3.3 Methodology

1. Assessment and Planning: The methodology begins with a thorough assessment of the organization's current identity and access management (IAM) infrastructure, including on-premises Active Directory, existing identity providers, and cloud services. This assessment helps identify existing challenges, requirements, and goals for implementing Azure Active Directory (Azure AD). Based on the assessment findings, a detailed implementation plan is developed, outlining migration strategies, integration requirements, security considerations, and timeline for deployment.
2. Deployment and Configuration: Once the implementation plan is finalized, the deployment phase begins with provisioning Azure AD tenants, configuring directory settings, and synchronizing user identities from on-premises Active Directory to Azure AD using tools such as Azure AD Connect. During this phase, authentication methods, access policies, and security controls are configured to align with organizational requirements and best practices. Integration with existing applications, services, and identity providers is also established to ensure seamless access and interoperability.
3. Testing and Validation: After deployment and configuration, thorough testing and validation of the Azure AD environment are conducted to ensure that all components function as intended and meet the organization's requirements. This includes testing user authentication, access control policies, single sign-on (SSO), multi-factor authentication (MFA), and integration with cloud services and applications. Any issues or discrepancies identified during testing are addressed and resolved before proceeding to production deployment.
4. Training and Adoption: As the Azure AD environment is deployed and validated, training and adoption efforts are initiated to familiarize users, administrators, and IT staff with the new identity and access management solution. Training sessions cover topics such as user authentication, self-service password reset, access requests, and security best practices. Additionally, documentation and resources are provided to support ongoing adoption and usage of Azure AD features and functionalities.

5. Monitoring and Optimization: Once Azure AD is in production, continuous monitoring and optimization are essential to ensure the ongoing security, performance, and efficiency of the identity and access management environment. Monitoring tools and dashboards are utilized to track user activity, detect security incidents, and identify areas for improvement. Regular reviews and audits of access controls, security policies, and compliance requirements are conducted to address evolving threats and regulatory changes. Additionally, optimization efforts focus on refining configuration settings, adjusting access policies, and incorporating feedback from users and administrators to enhance the overall effectiveness of Azure AD.

CHAPTER-4

DEPLOYMENT OPTIONS

4.1 Types of Deployment Options

Azure Active Directory (Azure AD) offers flexibility in deployment, allowing organizations to choose the deployment model that best fits their requirements

1. **Cloud-Only Deployment:** In a cloud-only deployment, Azure AD serves as the primary identity and access management solution without reliance on on-premises infrastructure. Organizations manage user identities, access policies, and security settings entirely within the Azure AD portal.This deployment model is suitable for organizations with a cloud-first strategy, startups, or thosewithout an existing on-premises Active Directory infrastructure.

2. **Hybrid Identity with On-Premises Active Directory:** Many organizations have an existing on-premises Active Directory infrastructure managing user identities and access to resources. Azure AD offers seamless integration with on-premises Active Directory through Azure AD Connect, a tool that synchronizes on-premises directory objects with Azure AD. With hybrid identity, organizations can leverage their existing investments in on-premises identity infrastructure while extending identity management to cloud services. Users can enjoy a unified login experience across both cloud and on-premises resources, enhancing productivity and security.

3. **Integration with Microsoft 365 and Other Microsoft Cloud Services:** Azure AD is tightly integrated with Microsoft 365 (formerly Office 365) and other Microsoft cloud services. Organizations subscribing to Microsoft 365 automatically gain access to Azure AD services for user authentication, access control, and security. Azure AD provides seamless access to Microsoft cloud applications such as Exchange Online, SharePoint Online, Teams, and more, simplifying user management and access control.

4.2 Azure Active Directory Components

Fig 4.2.1: Azure Active Directory Components

- **Directory Data** is the data stored for your directory system. The directory data is created from the identity and access data provided by your organization to populate the service. This data includes the following entities and their attributes: Users, groups and group memberships, devices, applications, and roles. Directory Data alsoincludes the metadata necessary to represent the relationships between these objects;some of which is provided by the customer and some of which is created by Azure AD services based on user actions such as registering applications, joining devices, etc.
- **Core Store** is the complete set of an organization's Directory Data is stored in a logical container (a "tenant") in a specific scale unit in the Azure AD distributed datastore. The Azure AD storage is divided into scale units, and each unique scale unit holds multiple tenants. The Azure AD core store also provides the directory data access interfaces to other services.

- **Authentication Services:** Processes user input, validates credentials, and implements the authentication flows, endpoints, and security tokens required by the differentt industry standards supported by the system industry standards supported by the system. The industry standards define the formatand exchange patterns for issuing, renewing, canceling, and validating security tokens provided by the authentication services as a security token service (STS).

- **Identity Security and Protection Services**: Provides identity-driven protection to users when interacting with the system such as Azure Multifactor Authentication (MFA), Azure AD Identity Protection, and Conditional Access.
- **Identity and Access Management (IAM) Services:** Provides advanced identity management features such as self-service password reset, self-service group management, dynamic group.
- **Azure AD Services:** Provides customers the infrastructure necessary to integrate existing onpremises infrastructure to Azure AD

a) **Azure AD Connect** provides synchronization of on-premises directory users to the cloud.

b) **Azure AD Connect Health** provides monitoring and analytics for synchronization, federation, and domain services.

c) **Azure AD Application Proxy** enables secure publishing of on-premises web applications for remote access

d) **Azure AD Domain Services** Provides managed domain services, such as domain join, group policy, LDAP, Kerberos, and NTLM authentication. These services are fully compatible with Windows Server Active Directory.

- **Azure AD Identity Governance**: Provides customers governance capabilities such as Azure AD Privileged Identity Management (PIM) Just In time (JIT) access to privileged roles, access certification, attestation campaigns, alerting, and reporting.
- **Azure AD External Identities:** Provides authentication services for external identities, such as users in partner organizations or consumers.

CHAPTER-5

ADVANTAGES, DISADVANTAGES & APPLICATIONS

5.1 ADVANTAGES

- **Centralized Identity Management:** Azure AD provides a centralized platform for managing useridentities, access controls, and security policies across cloud and on-premises environments, simplifying administration and reducing management overhead.
- **Seamless Integration with Microsoft Services:** Azure AD seamlessly integrates with Microsoft 365, Azure services, and other Microsoft products, enabling users to access a wide range of applications and services with a single set of credentials, enhancing productivity and user experience.
- **Scalability and Flexibility**: Azure AD is highly scalable, capable of supporting organizations of all sizes, from small businesses to large enterprises. It offers flexible deployment options, including cloud-only, hybrid, and federated identity models, to accommodate diverse IT environments and business needs.
- **Enhanced Security Features:** Azure AD offers advanced security features such as multi-factor authentication (MFA), conditional access policies, identity protection, and risk-based authentication, helping organizations protect against security threats and ensure compliance with regulatory requirements.
- **Cost-Effective Solution:** Azure AD is available as a subscription-based service with flexible pricing plans, allowing organizations to pay only for the features and resources they use. This makes it a cost-effective solution for implementing robust identity and access management capabilities without significant upfront investment.

5.2 DISADVANTAGES

- **Complexity of Configuration:** Configuring Azure AD can be complex, especially for organizations with complex IT environments or specific customization requirements. Proper planning and expertise are required to ensure that Azure AD is configured correctly and meets the organization's needs.
- **Dependency on Internet Connectivity:** Azure AD relies on internet connectivity for authentication and access control, which can pose challenges in environments with unreliable or limited internet connectivity. Organizations need to have contingency plans in place to ensure uninterrupted access to resources.
- **Potential for Service Disruptions:** Like any cloud-based service, Azure AD is susceptible to service disruptions or outages, which can impact user access and productivity. Organizations should have backup authentication methods and contingency plans in place to mitigate the impactof service disruptions.

5.3 APPLICATIONS

- **User Authentication and Access Management: Azure**: AD serves as a centralized identity management platform, allowing organizations to authenticate and authorize users to access applications and resources.
- **Cloud Application Integration:** Azure AD enables seamless integration with a wide range of cloud-based applications, including Microsoft 365 (formerly Office 365), Salesforce, Dropbox, and more.
- **Identity Protection and Security:** Azure AD offers advanced security features to protect against identity-related threats, such as phishing attacks, account compromise, and insider threats.
- **Business-to-Business (B2B) Collaboration:** Azure AD B2B enables secure collaboration with external partners, suppliers, and customers by providing them with access to shared resources and applications
- **Business-to-Customer (B2C) Identity Management:** Azure AD B2C allows organizations to manage customer identities and enable secure authentication for customer-facing applications and services.
- **Compliance and Reporting:** Azure AD offers reporting and auditing capabilities to help organizations monitor user activities, access patterns, and security events

CHAPTER-6

CONCLUSION

6.1 Conclusion

In conclusion, Azure Active Directory (Azure AD) stands as a robust and versatile identity and access management solution that offers numerous advantages for organizations seeking to streamline operations, enhance security, and improve user experience. Through its centralized identity management, seamless integration with Microsoft services, scalability, and advanced security features, Azure AD empowers organizations to efficiently manage user identities, control access to resources, and enforce security policies across cloud and on-premises environments. While Azure AD presents several advantages, it is not without its challenges, including complexity of configuration, dependency on internet connectivity, and potential service disruptions. Scope and Limitations

6.1.1 Scope

- **Cross-Platform Integration**: Azure AD offers extensive support for integrating with a wide range of platforms, including Microsoft services, third-party applications, and on-premises infrastructure, enabling organizations to centralize identity management and access controls across heterogeneous environments.
- **Enhanced Security and Compliance:** With advanced security features such as multi-factor authentication (MFA), conditional access policies, and identity protection, Azure AD provides organizations with the tools they need to strengthen security posture, mitigate risks, and ensure compliance with regulatory requirements.

Limitations

- Complexity of configuration and customization options.
- Dependency on internet connectivity for authentication and access control.

6.2 Future Enhancement

- Enhanced support for hybrid identity scenarios, facilitating seamless integration between on-premises Active Directory and Azure AD.
- Integration with emerging authentication methods such as biometric authentication and passwordless authentication for improved security and user experience.
- Expansion of identity governance capabilities, including more granular access controls, automated access reviews, and compliance reporting.
- Integration with advanced threat protection solutions to enhance detection and response capabilities for identity-based security threats.
- Continued innovation in identity management features to address evolving security challenges and regulatory requirements.

REFERENCES

[1] Microsoft Azure Active Directory, Microsoft Documentation. Available: https://docs.microsoft.com/en-us/azure/active-directory/

[2] "Azure Active Directory: What Is It and How Does It Work?", by Ryan Brooks, Okta. Available: https://www.okta.com/identity-101/azure-active-directory/

[3] "Azure Active Directory: Overview and Getting Started", by Richard Hay, Petri. Available: https://petri.com/azure-active-directory-overview-getting-started

[4] "Top 10 Benefits of Azure Active Directory", by Joy Adams, Cimatri. Available: https://www.cimatri.com/blog/top-10-benefits-of-azure-active-directory

[5] "Azure Active Directory: Features, Pricing, Alternatives", by Louie Andre, Software Advice. Available: https://www.softwareadvice.com/hr/azure-active-directory-profile/

[6] "Azure AD vs. Active Directory: What's the Difference?", by Kunal Grover, ManageEngine. Available: https://blogs.manageengine.com/active-directory/2019/07/30/azure-ad-vs-active- directory-whats-the-difference.html

[7] "Azure Active Directory: The Total Cost of Ownership", by Brad Sams, Petri. Available: https://petri.com/azure-active-directory-the-total-cost-of-ownership

[8] "How to Implement Azure Active Directory?", by Andrew Bryant, Softchoice. Available: https://www.softchoice.com/blogs/azure/how-to-implement-azure-active-directory

[9] "Azure Active Directory: Benefits, Features, and How It Works", by Marko Aleksic, phoenixNAP. Available: https://phoenixnap.com/blog/azure-active-directory

[10] "Azure Active Directory: What It Is and Why You Should Use It", by Andy Syrewicze, Altaro. Available: https://www.altaro.com/msp-dojo/azure-active-directory-overview/

[11] "Getting Started with Azure Active Directory", by Todd Klindt, Pluralsight. Available: https://www.pluralsight.com/courses/getting-started-azure-active-directory

[12] "Understanding Azure Active Directory", by Joe Palarchio, Perficient. Available: https://blogs.perficient.com/2018/08/06/understanding-azure-active-directory/

[13] "Azure Active Directory: Key Features and Benefits", by Lisa St. Clair, CDW. Available: https://www.cdw.com/content/cdw/en/articles/cloud-computing/2021/05/03/azure-active- directory-key-features-benefits.html

[14] "Azure Active Directory: A Comprehensive Guide", by Sarah Lean, Microsoft MVP. Available: https://pixelrobots.co.uk/2021/03/azure-active-directory-a-comprehensive-guide/

[15] "Azure Active Directory: The Ultimate Guide", by Aram Koukia, Lucidchart. Available: https://www.lucidchart.com/blog/azure-active-directory-the-ultimate-guide