*International Journal on Advances in Engineering Technology and Science*
*Volume: 5, Issue: 1, 2024, e-ISSN: 2455-3131*
*DOI: 10.5281/zenodo.10621038*

# Rise of Identity and Access Management with Microsoft Security

Sheetakshi Shukla[1], Kirti Jain[2]

[1]Research scholar, School of Advanced Computer, Sanjeev Agrawal Global Educational University, Bhopal
[2]Associate Professor, Sanjeev Agrawal Global Educational University, Bhopal

[1]Sheetakshi11@gmail.com
[2]kirti.j@sageuniversity.edu.in

*Abstract* – **Identity and Access Management (IAM) is a pivotal element in modern cybersecurity strategies, enabling organizations to manage user identities and control access to digital resources securely. This paper focuses on Microsoft's comprehensive suite of IAM solutions, emphasizing the innovative capabilities of Microsoft Entra ID as a central component within its ecosystem. The discussion spans Entra ID's role in IAM, Multi-Factor Authentication (MFA), Conditional Access policies, and Microsoft Entra Privileged Identity Management (PIM). This research explores the dynamic landscape of IAM in the context of Microsoft security, addressing challenges and opportunities posed by contemporary cybersecurity threats and evolving work environments. Key topics include the integration of IAM solutions with Microsoft 365 services, the impact of remote work on identity governance, and the effective implementation of conditional access policies to enhance security without compromising user experience [1]. Furthermore, the paper investigates the role of IAM, specifically Microsoft Entra ID, in meeting security and compliance requirements. It delves into data protection, threat intelligence, and compliance reporting within the Entra ID framework. As organizations navigate hybrid environments that span on-premises and cloud infrastructures, the research examines the intricacies of managing user authentication in such diverse setups. The study concludes by emphasizing the importance of adapting IAM strategies continuously to address evolving cybersecurity challenges within Microsoft's security ecosystem. By referencing the latest Microsoft Entra ID documentation and industry best practices, this research contributes to a deeper understanding of the significance of IAM, specifically Microsoft Entra ID, and its practical implications for organizations seeking robust identity and access management solutions [2].**

***Keywords*** **– IAM, Microsoft Entra ID, MFA, Conditional Access, Identity Governance.**

## I. INTRODUCTION

### A. *Definition of Identity and Access Management (IAM).*

Identity and access Management refers to the solutions for the entire Access and Authorization along with Identity verifications. That too with the Identity Modernization. Identity and Access Management (IAM) is a critical component of modern cybersecurity strategies, encompassing the policies, technologies, and processes that organizations use to manage and secure digital identities and control access to their resources. In today's interconnected and digital landscape, effective IAM is essential for safeguarding sensitive data, ensuring regulatory compliance, and mitigating the risk of unauthorized access. Microsoft Security offers a comprehensive suite of IAM solutions designed to address the evolving challenges of identity management in the digital age. At its core, Microsoft's IAM framework aims to provide seamless yet secure access to resources, applications, and data for authorized users while preventing unauthorized access. Key components of Microsoft's IAM include Entra ID, which serves as a cloud-based identity and access management service. Entra ID enables organizations to centralize identity management, streamline authentication processes, and enforce access policies across various applications and services. Leveraging features such as Multi-Factor Authentication (MFA) and Conditional Access, organizations can enhance the security posture of their environments and protect against identity-based threats.

Furthermore, Microsoft's IAM extends to on-premises environments through Active Directory, providing a bridge between traditional and cloud-based identity management. The integration of on-premises and cloud-based IAM solutions allows for a unified and cohesive approach to identity and access management. As organizations navigate the complexities of IAM, Microsoft's commitment to continuous innovation is evident in its efforts to address emerging security challenges. The ongoing development of advanced threat detection, identity protection, and privileged access management features demonstrates Microsoft's dedication to staying at the forefront of IAM best practices [1-3].

### B. *Importance of IAM in today's digital landscape.*

Identity and Access Management (IAM) holds paramount significance in today's digital landscape, serving as a linchpin for cybersecurity strategies. In the context of Microsoft Security, IAM plays a pivotal role in addressing the evolving challenges of identity management and access control. Several key aspects underscore the importance of IAM in the current digital era, especially when integrated with Microsoft's security solutions:

*Protecting Against Unauthorized Access:*

IAM serves as the first line of defense against unauthorized access to sensitive data, applications, and resources. Microsoft's IAM solutions, such as Entra ID, employ robust authentication mechanisms, including Multi-Factor Authentication (MFA), to ensure that only authorized users gain access.

*Adapting to a Hybrid Environment:*

In the modern business landscape, organizations often operate in hybrid environments, with a mix of on-premises and cloud-based resources. Microsoft's IAM solutions seamlessly bridge this gap, providing a unified approach to identity management that spans both traditional Active Directory and cloud-based Entra ID.

*Enhancing Security Posture:*

IAM is integral to bolstering the overall security posture of an organization. Microsoft's IAM solutions offer advanced features like Conditional Access, which enables organizations to enforce policies based on various factors such as user location, device health, and risk level. This ensures that access controls dynamically adapt to the evolving threat landscape.

*Mitigating Insider Threats:*

IAM plays a crucial role in mitigating insider threats by enforcing the principle of least privilege. Microsoft Security solutions, integrated with IAM, allow organizations to define and enforce access policies based on roles and responsibilities, reducing the risk of unauthorized access or data breaches from within the organization.

*Streamlining Compliance Management:*

In an era of stringent data protection regulations, IAM becomes a linchpin for compliance management. Microsoft's IAM solutions provide tools and features to help organizations adhere to regulatory requirements, manage user identities securely, and audit access to sensitive information.

*Facilitating Productivity and Collaboration:*

IAM is not just about security; it's also about enabling seamless user experiences. Microsoft's IAM solutions are designed to provide secure and convenient access to resources, fostering productivity and collaboration while maintaining the necessary security controls.

*Continuous Innovation and Threat Detection:*

Microsoft is committed to staying ahead of emerging threats. IAM solutions, integrated into the broader Microsoft Security ecosystem, benefit from continuous innovation in threat detection, identity protection, and privileged access management. This ensures that organizations can proactively address new and evolving security challenges [4].

### *C. Introduction to Microsoft Security and its role in IAM.*

In the rapidly evolving landscape of cybersecurity, Microsoft Security stands as a comprehensive suite of tools and solutions designed to safeguard digital environments. At the core of Microsoft Security is the recognition that effective Identity and Access Management (IAM) is fundamental to building a robust defense against evolving threats. IAM within the Microsoft Security framework encompasses a range of technologies and practices aimed at securely managing digital identities and controlling access to critical resources.

Microsoft Security Overview: Microsoft Security represents a holistic approach to cybersecurity, offering a suite of interconnected solutions to protect against a diverse array of threats. From endpoint protection to cloud security, Microsoft Security is designed to provide a cohesive and integrated defense strategy for organizations operating in today's complex digital ecosystems [5].

IAM in the Microsoft Security Ecosystem: IAM serves as a cornerstone within Microsoft Security, addressing the challenges associated with identity management and access control. Microsoft's IAM solutions seamlessly integrate with other security components to create a unified defense mechanism. Key components include:

*Entra ID:* Entra ID is Microsoft's cloud-based IAM service, centralizing identity management across cloud and on-premises environments. It facilitates secure and seamless access to applications and resources, incorporating advanced features such as Multi-Factor Authentication (MFA) and Conditional Access to enhance security.

*Active Directory (AD):* Active Directory remains a foundational element in IAM, bridging on-premises and cloud environments. It enables organizations to manage user identities, enforce access policies, and integrate with other Microsoft Security solutions for a cohesive defence strategy.

*Entra ID Protection:* Entra ID Protection is a critical component that leverages advanced analytics to detect and respond to identity-based threats. It helps organizations identify risky sign-ins and unusual behaviour, allowing for proactive mitigation of potential security incidents.

Microsoft Defender for Identity: Formerly known as Azure Advanced Threat Protection, Microsoft Defender for Identity provides advanced threat detection capabilities within an organization's on-premises Active Directory. It focuses on detecting and investigating identity-based attacks in real-time.

Privileged Identity Management (PIM): PIM within Entra ID offers just-in-time privileged access, ensuring that users have elevated access only when needed. This minimizes the risk associated with prolonged elevated privileges, addressing a common attack vector [6-10].

Role of Microsoft Security in IAM: Microsoft Security plays a pivotal role in shaping and reinforcing IAM strategies. By integrating IAM seamlessly into the broader security landscape, Microsoft enables organizations to:

Strengthen Security Posture: Microsoft Security, with its IAM components, empowers organizations to enforce strong access controls, reduce the risk of unauthorized access, and proactively respond to identity-based threats.

Facilitate Compliance: The integrated IAM solutions assist organizations in meeting regulatory compliance requirements by providing tools for secure identity management, access auditing, and policy enforcement.

Adapt to Modern Work Environments: In a landscape characterized by remote work and cloud adoption, Microsoft Security's IAM solutions cater to the dynamic needs of modern workplaces, offering secure access to resources from anywhere.

Innovate Against Emerging Threats: Microsoft's commitment to continuous innovation ensures that IAM solutions within the Microsoft Security ecosystem stay ahead of emerging threats, incorporating advanced technologies to protect against evolving attack vectors.

## II. EVOLUTİON OF IAM

### *A. The traditional approach to IAM and its limitations.*

The traditional approach to Identity and Access Management (IAM) has been characterized by on-premises solutions, manual processes, and a focus on securing network perimeters. While this approach served well in the past, it has notable limitations in addressing the challenges posed by the evolving digital landscape. Here are some key aspects of the traditional IAM approach and its limitations:

Perimeter-Centric Security: Traditional IAM often relies on the concept of a network perimeter, assuming that securing the boundary of the network is sufficient. In today's scenario, where users access resources from various locations and devices, this approach is no longer effective. It does not account for the reality of remote work, mobile devices, and cloud-based services.

User-Centric Security: The traditional approach tends to focus on securing the user's identity within the corporate network. However, as organizations adopt cloud services and collaboration tools, users need to access resources beyond the corporate perimeter. Traditional IAM may struggle to provide seamless and secure access in these distributed environments.

Complexity and Inefficiency: On-premises IAM solutions can be complex to manage, requiring significant manual effort for tasks such as user provisioning, de-provisioning, and role management. This complexity can lead to inefficiencies, delays, and an increased risk of errors in maintaining accurate and up-to-date user access.

Limited Flexibility and Scalability: Traditional IAM systems may lack the agility needed to adapt to changing business requirements. Scaling the IAM infrastructure to accommodate new users, applications, or services can be challenging and may involve significant upfront costs and lead times.

Inadequate Authentication Methods: Many traditional IAM systems rely heavily on username-password combinations for authentication. This method is susceptible to various security threats, such as phishing and password-based attacks. Single-factor authentication, commonly used in traditional IAM, is becoming insufficient in today's threat landscape.

Difficulty in Managing Privileged Access: The traditional IAM approach may face challenges in effectively managing privileged access. Static access privileges for administrators and other high-privileged users can create security vulnerabilities, especially if these privileges are not regularly reviewed and updated.

Insufficient Visibility and Monitoring: Traditional IAM systems may lack comprehensive visibility into user activities and behavior. This limitation hampers the ability to detect anomalous patterns that could indicate a security threat. Monitoring and auditing capabilities may be inadequate for identifying and responding to security incidents promptly.

Regulatory Compliance Challenges: As regulatory requirements become more stringent, traditional IAM systems may struggle to keep up with compliance mandates. The lack of advanced reporting and auditing features can hinder organizations in demonstrating and maintaining compliance with industry regulations [2].

### *B. The emergence of Microsoft's IAM solutions.*

The emergence of Microsoft's Identity and Access Management (IAM) solutions represents a significant evolution in the field of cybersecurity, aligning with the changing dynamics of modern digital environments. Microsoft has played a pivotal role in shaping IAM practices, offering a suite of integrated solutions that address the challenges posed by cloud computing, remote work, and the increasing sophistication of cyber threats. Here is an overview of the emergence of Microsoft's IAM solutions:

Shift to Cloud Computing: As organizations transitioned from traditional on-premises IT infrastructure to cloud-based services, Microsoft recognized the need for IAM solutions that could seamlessly bridge on-premises and cloud environments. The shift to cloud computing brought forth new challenges related to identity management, authentication, and access control.

*Entra ID:* Entra ID emerged as a cornerstone of Microsoft's IAM strategy. Launched as a cloud-based identity and access management service, Entra ID enables organizations to centralize and manage identities across cloud and on-premises environments. It provides a scalable and secure solution for user authentication, single sign-on, and access governance.

*Integration with Office 365 and Azure Services:* Microsoft's IAM solutions are deeply integrated with popular cloud services such as Office 365 and Azure. This integration allows organizations to leverage a unified identity platform for accessing a diverse range of applications, data, and resources, promoting a seamless and secure user experience.

*Multi-Factor Authentication (MFA) and Conditional Access:* Recognizing the limitations of traditional authentication methods, Microsoft introduced MFA as a standard feature in Entra ID. MFA enhances security by requiring users to provide multiple forms of verification. Conditional Access allows organizations to set policies based on various parameters, including user location, device health, and risk level, thereby enabling adaptive access controls.

*Advanced Threat Protection for Identity:* Microsoft has invested heavily in developing advanced threat protection capabilities within its IAM solutions. Features such as Entra ID Protection and Microsoft Defender for Identity use machine learning and analytics to detect and respond to identity-based threats in real-time, enhancing the overall security posture.

*Privileged Identity Management (PIM):* Microsoft's IAM suite includes PIM, a solution that focuses on managing and monitoring privileged access. PIM helps organizations enforce just-in-time privileged access, reducing the risk associated with prolonged elevated privileges and enhancing control over critical systems and resources.

*User-Friendly Self-Service:* Recognizing the importance of user experience, Microsoft has incorporated user-friendly self-service capabilities into its IAM solutions. Users can manage their own identities, reset passwords, and perform other routine tasks, reducing the burden on IT administrators and improving overall efficiency.

*Compliance and Reporting Tools:* Microsoft's IAM solutions include robust compliance and reporting tools that assist organizations in meeting regulatory requirements. These tools provide audit logs, reports, and insights into user access, helping organizations demonstrate compliance with industry standards [6-10].

## III. MİCROSOFT SECURİTY AND IAM

### A. *Overview of Microsoft's IAM solutions, including Entra ID and Entra ID Protection.*

Microsoft's Identity and Access Management (IAM) solutions play a crucial role in securing digital identities and controlling access to resources. Two key components of Microsoft's IAM offerings are Entra ID and Entra Identity Protection.

*Microsoft Entra ID:*

Entra ID is Microsoft's cloud-based identity and access management service that provides a robust foundation for secure and seamless access to applications and resources. It serves as a central identity platform, supporting both on-premises and cloud environments. Entra ID is an integral part of the broader Microsoft 365 and Azure ecosystems.

*Key Features:*

Single Sign-On (SSO): Entra ID enables users to sign in once and access a variety of applications without the need for multiple credentials.

Multi-Factor Authentication (MFA): Enhances security by requiring users to provide additional verification factors beyond passwords.

Conditional Access: Allows organizations to define access policies based on various conditions, such as user location, device health, and risk level.

Identity Protection: Integrates with Entra Identity Protection to detect and respond to identity-based threats.

*Use Cases:*

User Authentication: Entra ID provides secure and convenient authentication for users across different applications and services.

Access Control: Organizations can enforce access policies and controls to ensure that users have the appropriate level of access based on their roles and responsibilities.

*Entra Identity Protection:*

Overview: Entra Identity Protection is a specialized feature within Entra ID designed to enhance the security of identities by leveraging advanced analytics and machine learning. It focuses on detecting and responding to identity-based threats in real-time, helping organizations proactively mitigate potential security risks.

*Key Features:*

Risk-Based Conditional Access: Evaluates user sign-ins in real-time, assigning a risk level based on various factors. Organizations can then define conditional access policies to respond to high-risk events.

User Risk Policies: Detects anomalous behavior that may indicate a compromised account or identity and triggers alerts or remediation actions.

Sign-In Risk Policies: Analyzes the risk associated with each sign-in attempt, factoring in user behavior, device health, and other contextual data.

### B. *Integration of IAM with other Microsoft security products, such as Microsoft Defender for Identity.*

Microsoft Defender for Identity (formerly known as Azure Advanced Threat Protection) is a cloud-based security solution that helps organizations detect and respond to advanced identity-related threats, including identity compromise and lateral movement.

*Integration Points:*

User and Entity Behavioral Analytics (UEBA): Defender for Identity leverages UEBA to analyze user behavior and entity interactions, creating a baseline of normal activity. This includes the analysis of login patterns, file access, and other activities associated with user identities.

Integration with Entra ID: Defender for Identity seamlessly integrates with Entra ID to enhance its threat detection capabilities. This integration enables a comprehensive view of user identities and their activities across on-premises and cloud environments.

Risk-Based Conditional Access: Defender for Identity's risk assessment data can be used in conjunction with Entra ID Conditional Access policies. High-risk events detected by Defender for Identity can trigger adaptive access controls, providing an additional layer of security.

Incident Investigation and Response: When Defender for Identity detects suspicious activity, security teams can use its incident investigation features to gain insights into the scope and impact of the threat. This helps organizations respond effectively to security incidents.

Integration with Microsoft Cloud App Security: Defender for Identity integrates with Microsoft Cloud App Security to extend threat detection and protection to cloud applications, ensuring a holistic approach to securing identity and data.

*Benefits of Integration:*

Unified Threat Detection: The integration allows for a unified approach to threat detection by combining insights from Defender for Identity with IAM capabilities, offering a more comprehensive view of potential risks.

Adaptive Access Controls: High-risk events detected by Defender for Identity can dynamically influence access controls defined in Entr ID Conditional Access policies, enabling adaptive responses to security threats.

Incident Response: Security teams can efficiently investigate and respond to incidents by correlating identity-related threat data from Defender for Identity with Entra ID activities.

Holistic Cloud and On-Premises Security: The integration ensures that both cloud-based and on-premises environments benefit from a unified IAM and threat detection strategy.

The integration of IAM with Microsoft Defender for Identity creates a synergistic approach to cybersecurity, aligning identity management with advanced threat detection and response capabilities. This unified strategy is essential in the modern threat landscape, where identity compromise is a common vector for cyberattacks.

### C. *Benefits of using Microsoft Security for IAM, such as centralized management and enhanced security measures.*

Utilizing Entra ID for Identity and Access Management (IAM) offers numerous advantages, combining centralized administration with heightened security measures. Entra ID acts as a centralized identity hub, streamlining user management across on-premises and cloud environments. The seamless integration of Entra ID with the broader Entra ecosystem ensures consistent IAM policies across applications and services.

Security is fortified through Entra ID's robust features, including Multi-Factor Authentication (MFA) and Conditional Access. MFA adds an extra layer of authentication, while Conditional Access enables organizations to enforce access policies based on user context and risk level. This layered security approach enhances protection against evolving threats.

Entra ID's advanced threat detection, such as Entra ID Identity Protection, utilizes machine learning to swiftly identify and respond to identity-based threats, ensuring a unified approach to threat detection. Additionally, Entra ID's Privileged Identity Management (PIM) facilitates just-in-time privileged access, minimizing the risks associated with prolonged elevated privileges.

The user experience is streamlined through user-friendly self-service capabilities, empowering users to manage their own identities efficiently. Compliance management is enhanced with comprehensive reporting and auditing tools, supporting organizations in meeting regulatory requirements.

In adapting to modern work environments, Entra ID's flexibility accommodates hybrid infrastructures seamlessly, ensuring a secure and cohesive user experience across both cloud and on-premises environments. In essence, leveraging Entra ID for IAM creates a unified, adaptive, and secure framework that aligns with the dynamic demands of the digital landscape.

## IV. KEY FEATURES AND CAPABİLİTİES OF MİCROSOFT SECURİTY IAM

### A. *Single sign-on (SSO) functionality for seamless access to multiple applications.*

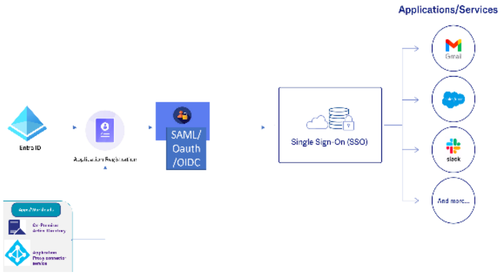

Figure 1 SSO for ON-Prem Application

For on-premises applications, the Entra ID’s app proxy application is utilized to onboard the applications to the cloud. This involves an app registration process where the on-premises application is connected to Entra ID. Once the application is successfully onboarded to the cloud, users can access the application through the cloud environment. When a user attempts to access the application, they are directed to the SSO process, which utilizes industry-standard protocols such as SAML (Security Assertion Markup Language), OIDC (OpenID Connect), or OAuth (Open Authorization).

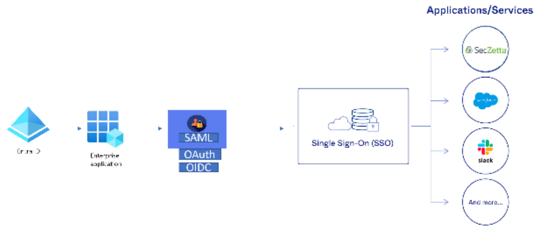

Figure 2 SSO for Cloud Application

For cloud-based applications, the workflow begins with the configuration of the application through the enterprise applications feature in Azure. The choice of authentication method, whether it's SAML-based, OAuth 2.0, or OIDC, depends on the support provided by the application and is selected by the administrator. Once the application setup is completed, the SSO configuration is performed through the Azure portal. This involves configuring the SSO settings specific to the application, such as identity provider configuration and claims mapping. After the SSO setup is finalized, users can access the application with SSO. They simply select the application from their portal or application launcher, and they are automatically authenticated using their existing credentials, eliminating the need to enter their password again.

### B. *Multi-factor authentication (MFA) options to enhance user verification.*

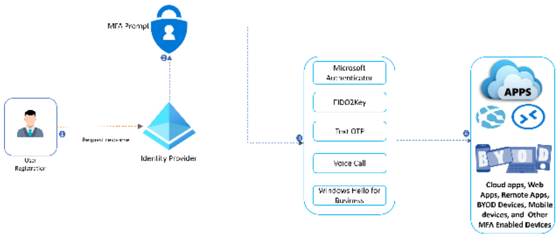
MFA Prompt
User Registration
Request response
Identity Provider
Microsoft Authenticator
FIDO2Key
Text OTP
Voice Call
Windows Hello for Business
APPS
BYOD
Cloud apps, Web Apps, Remote Apps, BYOD Devices, Mobile devices, and Other MFA Enabled Devices

Figure 3 Entra ID MFA

Users initiate the registration process for Multi-Factor Authentication (MFA). MFA provides an additional layer of security by requiring users to provide multiple forms of verification when accessing resources.

The user begins by initiating the MFA registration process, typically through a self-service portal or user account settings. During the registration, the user is guided through the setup process, which may include providing contact information and selecting preferred MFA methods.

Once the registration is complete, the user is redirected to the login page. When attempting to log in, the user enters their single factor, typically their username and password. After entering the single factor, the user is then redirected to the MFA prompt.

### C. *Role-based access control (RBAC) for efficient management of user permissions.*

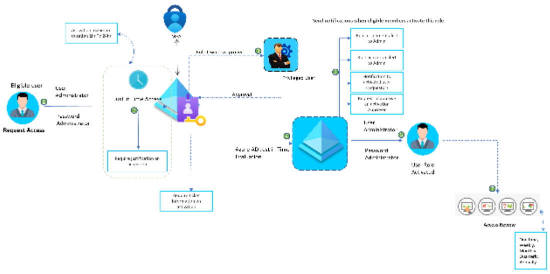

Figure 4 RBAC for Azure

The diagram depicts the user's eligibility for the user administrator and password administrator roles, which grant them the necessary privileges to carry out their responsibilities efficiently. This concept can be extended to M365 or Security groups as well. In addition, roles such as Global admin, domain admin, schema admin, backup operator, and enterprise admin are also applicable as part of the requirement to provide specific authorization levels for performing various tasks.

To activate the assigned role, the user initiates the activation process and provides a justification for the activation. The activation request is then redirected to the user's manager for approval. The manager reviews the request and decides whether to approve or deny it based on the user's job requirements and the principle of least privilege.

Once the activation request is approved, the user is granted just-in-time access to the assigned role. Just-in-time access ensures that privileged access is granted only when needed, reducing the risk of unauthorized access, and limiting the exposure of sensitive resources.

During the activation and subsequent role usage, logs are generated to track and monitor the user's activities. These logs serve as an important source of information for auditing purposes and enable IT administrators to detect any suspicious or anomalous behaviour. In the event of any unauthorized or unusual activity, alerts are triggered to the IT admin, allowing for timely investigation and response.

## V. CONCLUSION

In conclusion, Microsoft Security's IAM solutions, including PIM, MFA, Conditional Access, Identity Protection, SSO, and SSPR, form a robust and unified framework for securing identities and controlling access. PIM introduces just-in-time privileged access, MFA enhances authentication, and Conditional Access adapts access controls dynamically. Identity Protection employs advanced threat detection, while SSO streamlines user experiences. SSPR empowers users for efficient password management. Together, these components contribute to a secure, user-friendly, and compliance-focused IAM strategy, aligning with Microsoft Security's commitment to innovation in the ever-evolving landscape of cybersecurity.

## REFERENCES

[1] Aytaj Badirova, Shirin Dabbaghi, Faraz Fatami Moghaddam, Philip Modem, and Ramin Yohyapour, “A Survey on Identity and Access Management for Cross-Domain Dynamic Users: Issues, Solutions, and Challenges”, IEEE, Vol-11, pp 61660-61679, 24 May 2023.

[2] Sjoukje Zaal, “Azure Active Directory for Secure Application Development: Use modern authentication techniques to secure applications in Azure”, Packt Publishing, 2022.

[3] Timothy L. Warner, "Managing Identity and Access with Azure Active Directory," in Microsoft Azure for Dummies, Wiley, 2020, pp.229-249.

[4] Giuseppe Di Federico; Fabrizio Barcaroli, Cloud Identity Patterns and Strategies: Design enterprise cloud identity models with OAuth 2.0 and Azure Active Directory, Packt Publishing, 2022.

[5] Shimon Brathwaite, "Managing Identity and Access in Microsoft Azure," in MCA Microsoft Certified Associate Azure Security Engineer Study Guide: Exam AZ-500, Wiley, 2023, pp.29-72.

[6] Microsoft Document, “What is Azure Multifactor Authentication”, Oct 2023, Online, https://learn.microsoft.com/en-us/entra/identity/authentication/overview-authentication

[7] Microsoft Document, “What is SSO in Microsoft Entra ID”, Oct 2023, Online, https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-single-sign-on

[8] Microsoft Document, “What is Azure role-based access controls (RBAC)”, Aug 2023, Online, https://learn.microsoft.com/en-us/azure/role-based-access-control/overview.

[9] Kirti Jain, “Enhancing Cloud data security using Watermarking Technique” in Journal of Emerging Technologies and Innovative Research”, ISSN:2349-5162, Vol No. 9 Issue 7, July 2022.

[10] Microsoft Document, “What is Identity Protection”, Aug 2023, Online, https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

[11] Microsoft Document, “What is Privileged Identity Management?”, Aug 2023, Online, https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

[12] S. Ibrokhimov, K. L. Hui, A. Abdulhakim Al-Absi, h. j. lee and M. Sain, "Multi-Factor Authentication in Cyber Physical System: A State of Art Survey," 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South), 2019, pp. 279-284, doi: 10.23919/ICACT.2019.8701960.

[13] S. H. Khan and M. A. Akbar, "Multi-Factor Authentication on Cloud," 2015 International Conference on Digital Image Computing: Techniques and Applications (DICTA), Adelaide, SA, Australia, 2015, pp. 1-7, doi: 10.1109/DICTA.2015.7371288.

[14] N. Shaikh, K. Kasat and S. Jadhav, "Secured Authentication by Single Sign On (SSO): A Big Picture," 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2022, pp. 951-955, doi: 10.1109/ICCCIS56430.2022.10037708.

[15] San Murugesan; Irena Bojanova, "Identity and Access Management," in Encyclopedia of Cloud Computing , IEEE, 2016, pp.396-405, doi: 10.1002/9781118821930.ch33

[16] A. Sharma, S. Sharma and M. Dave, "Identity and access management- a comprehensive study," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 2015, pp. 1481-1485, doi: 10.1109/ICGCIoT.2015.7380701.

[17] S. B. Mallisetty, G. A. Tripuramallu, K. Kamada, P. Devineni, S. Kavitha and A. V. P. Krishna, "A Review on Cloud Security and Its Challenges," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2023, pp. 798-804, doi: 10.1109/IDCIoT56793.2023.10053520.

[18] Jeremy Moskowitz, "Set Up Azure AD and MDM," in MDM: Fundamentals, Security, and the Modern Desktop: Using Intune, Autopilot, and Azure to Manage, Deploy, and Secure Windows 10 , Wiley, 2019, pp.15-73, doi: 10.1002/9781119564362.ch2.

[19] J. Kadlec, D. Jaros and R. Kuchta, "Implementation of an Advanced Authentication Method within Microsoft Active Directory Network Services," 2010 6th International Conference on Wireless and Mobile Communications, Valencia, Spain, 2010, pp. 453-456, doi: 10.1109/ICWMC.2010.48.