National College of Ireland

Investigate access control models, and authentication mechanisms for a regulated industry based on Role-Based JIT Access Control using PIM and Biometrics in Azure AD

MSc Research Project
MSc Cyber Security

Shalini Jaganmohan
22201505

School of Computing
National College of Ireland

Supervisor: Michael Prior

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Shalini Jaganmohan
Student ID:	x22201505
Programme:	MSc in Cyber security **Year:** 2023-2024
Module:	MSc Research project
Supervisor:	Michael Prior
Submission Due Date:	12-08-2024
Project Title:	Investigate access control models, and authentication mechanisms for a regulated industry based on Role-based JIT access control using PIM and Biometrics in Azure AD
Word Count:	5995 **Page Count** 19

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Shalini Jaganmohan
Date:	11-08-2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Investigate access control models, and authentication mechanisms for a regulated industry based on Role-Based JIT Access Control using PIM and Biometrics in Azure AD

Shalini Jaganmohan
22201505

Abstract

Microsoft Azure Active Directory is a cloud-based identity and access management service offering application access control, directory services, and identity security. This research explores using role-based Just in Time (JIT) access control with Azure AD's Privileged Identity Management (PIM) and the Face API's biometric authentication to meet security and compliance needs in sectors like finance, healthcare, and government. The paper is hooked to PIM for user accounts, integrating Face API authentication for JIT access. It investigates in particular how rule-based access control can bring about additional security and compliance joined with facial recognition. Testing and evaluation are done at the very end of the research, which concludes that after creating and authenticating PIM user accounts, the user can schedule a team meeting or execute a task that needs approval based on JIT access control.

1 Introduction

The global cloud computing market is expected to grow rapidly in 2024 because there has been a sudden fast growth in cloud-based technologies and demand for scalable, flexible, and data-driven IT infrastructure. One of the leading providers of cloud computing services, Azure Active Directory (Azure AD) is the Microsoft identity and access management service in the cloud at the core of the Azure ecosystem organization in a regulated sector must manage access to sensitive information and crucial technology in a secure and compliant way. Traditional access control solutions can't accommodate many of these scenarios, which are highly dynamic and full of contextual variables. To rid the risk of unauthorized access and privileged account abuse, rule-based Just-In-Time Access Management has the potential to solve the problem.

Role-Based Access Control is a technique used in IAM where specific roles are assigned to individual users for the effective performance of job functions, with proper management over permissions and privileges. Such fine-grained access control helps in management, security, and creating a clean audit trail for compliance. It also provides very good scalability when the organization grows, since new roles can easily be added or modified without disruption to existing user assignments. On the other hand, Zero Trust is basically a 'deny all' position and enforces this default denial through a layered approach. This model is important to ensure that strong access controls are in place that will routinely and effectively deny attackers the capability to pivot laterally or scale their access within an environment. By implementing

RBAC in conjunction with Zero Trust principles, an organization can implement an end-to-end security framework that ensures sensitive data is protected and users have appropriate access to perform their roles effectively.(What is Just-in-Time Access (JIT)?)(Implementing Zero Trust with Microsoft Azure: Identity and Access Management (1 of 6) - Azure Government)

• PAM solutions constrain the time window in which one user is empowered to access an account. The rotation of credentials is performed once the user has signed into the account, or the elapsed time has expired.
• This ensures that the credentials are unknown to whoever has just used them, and privilege abuse is effectively eliminated.
• In more advanced JIT implementations, the PAM solution will rotate the passwords or shift accounts in and out of privileged groups on an as-needed basis, or even create brand new accounts and delete them at the end of the checkout window.
• JIT guards privileged access, even if an attacker could crack the password to an account. Since the JIT methodology has been implemented, the account would be worthless or non-existent.(What is Just-in-Time Access (JIT)?)

Passwordless authentication: It supports methods like FIDO2, including facial recognition and other biometrics like fingerprint scanning. This reduces dependency on traditional passwords that are easily breached and provides much more security and seamlessness in the login experience of the user. It reduces the risks of accidental or even intentional data breaches by allowing for visibility into and control over user access. Integrating Azure's capabilities for face authentication in already existing security systems will bring about improved entity and data security against unauthorized access and possible data breaches.

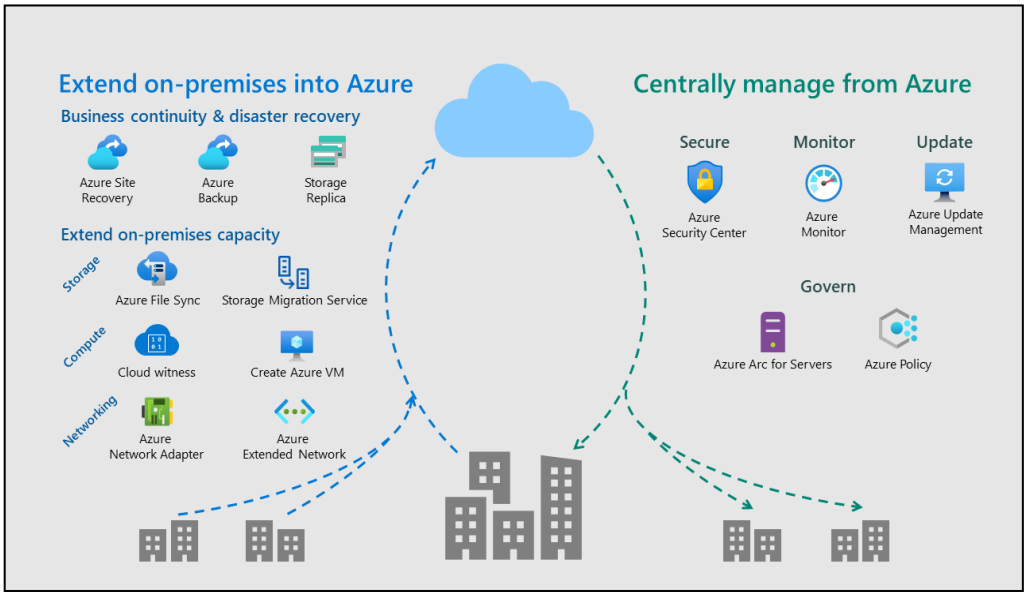

Figure 1: Microsoft Azure AD cloud platform

1.1 Research Question:

1. How can Rule-Based Just-In-Time Access Control, leveraging Privileged Identity Management and biometric authentication in Azure AD (Face API), enhance security and compliance in regulated industries?

This research aims to apply Microsoft Azure AD Privileged Identity Management (PIM) capability and the Face API to develop a strong rule-based JIT access control solution for certain relevant, regulated industries. Azure AD PIM centrally manages elevated access

privileges in an organization and allows organizations to provide temporary, time-limited access under preset rules and business requirements in an auditable way. If integrated with the Face API, the biometric identification feature in the facial recognition PIM role-based access-control feature would provide enhanced security, user convenience, and regulatory compliance. The use of a rule-based, just-in-time access control system allows an organisation to provide access based on dynamic, context-aware rules, including criteria about the identity of the subject, the location and device the subject is using, and risk criteria. This strategy reduces the risk of unauthorized access and any misuse of privileged accounts data breaches since users are granted no rights other than those necessary for their work.

2 Related Work

2.1 RBAC – Privileged Identity Management 'Just-In-Time' based research studies

In the paper, pascal cotret investigates "**JIT Compiler Security through Low-Cost RISC-V Extension,"(2023)**(Ducasse, Cotret and Lagadec, 2023) a new approach to enhance security in a Just-In-Time compiler has been proposed. This is essentially done with a low-cost RISC-V extension that makes the needed hardware available, which can practically enforce robust memory isolation mechanisms against code injection and data-only attacks. The authors provide experimental results proving the efficacy of this approach and underline its potential for low-overhead enhancement in security for JIT compilation processes within various applications. This work connects security instructions on RISC-V from JIT compiler-generated code to the processor.
It shows A RISC-V softcore processor with the RIMI security extension. A study of the extra instructions' impact on processor performance and intrusiveness.

Author Leandro Minku, states that **"JIT Fault Prevention, Motivated Modelling, and the Role of the User"**(Carver et al., 2020) argues that just-in-time fault prevention is necessary in software development, applying motivated modelling methodologies that adapt to user behaviours and system dynamics. Thus, the authors analyse different ways to adopt JIT fault prevention and underline how proactive approaches decrease the risk of software failure. They say that the knowledge of human motivations and interactions with the software system helps come up with successful error prevention models.

Saad EI Jaouhari proposed a paper "**A WebRTC/WoT-Based Health-Care Architecture Enhanced with Access Control**"(Jaouhari, Bouabdallah and Bonnin, 2018) introduces a novel architecture in design for projects on health care incorporated with WebRTC (Web Real-Time Communication) and the Web of Things, abbreviated as WoT. The proposed architecture, based on both real-time communication mechanisms enabled by WebRTC and the WoT established for device interconnectivity, will derive a scalable, adaptable, and suitable solution for the healthcare environments channelled in the paper. The implementation details related to the proposed access control measures toward data confidentiality and integrity maintenance, leading to potential applications of security effectiveness, are discussed.

The research was done by Yu Rong, an extension of the "**Research of extended RBAC model on permission control in the WEB information system"**(Liqing et al., 2011)**.** The authors aim to bring more flexibility and scalability to traditional systems of RBAC by incorporating further attributes into the access control mechanism. This extended model will allow more dynamic assignments of privileges among users through their attributes, based on the Just-In-

Time principles of access control. The paper thus provides foundational knowledge on how RBAC could be adapted to help modern security demands in web-based systems and contributes to the further research of access control frameworks which leverages JIT methodologies.

The second edition of Morey J. Haber and Darran Rolls's **“Identity Attack Vectors: Strategically Designing and Implementing Identity Security”**(Identity Attack Vectors: Strategically Designing and Implementing Identity Security, Second Edition) contextualizes the core place of identity security in modern cybersecurity frameworks. This new edition is a kind of response to the fast-changing threat landscape, in which identity has emerged as the number one target that cyber attackers gun for, hence the need to effectively manage identities and access. The authors demonstrate how poor identity hygiene can lead to large risks for organizations, which proves the need for an end-to-end strategy for securing identities throughout their lifecycle.

On January 16, 2020, **"CyberArk Expands Just-in-Time Capabilities Across Industry’s Broadest Privileged Access Management"**(CyberArk Expands Just-in-Time Capabilities Across Industry’s Broadest Privileged Access Management Portfolio - EBSCO) CyberArk announced that it was expanding its JIT access capabilities to strengthen its privileged access management portfolio. With this development, the company is seeking to curb a significant amount of risk that standing access exposes users to by providing temporary access to critical systems on demand. New additions to these features are short-lived SSH certificate authentication for Linux systems, allowing secure access without the hassle of constant credential management. Additionally, CyberArk's offerings now enable the temporary elevation of privileges for a range of operating systems, including Windows and Unix, and integrate with AWS to offer limited-privileged credentials.

2.2 Biometric authentication Microsoft Azure Face API-based research studies

According to B.V Satish Babu, this research study **“Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments (2024)”**(Satish Babu et al., 2024) brings to the foreground biometric authentication via facial recognition into access control systems tailored for IoT environments. Herein, a robust facial recognition algorithm is proposed, which utilizes deep learning to identify users with high accuracy under hard conditions of lighting and occlusions. The authors identify a dire need for improving IoT devices concerning security, placing major emphasis on fine user authentication in the protection of sensitive data and functionality.

The author Keshav Sharma, “**Advanced Bank Security and Management System**”(Sharma et al., 2022) has proposed an upgraded design to the current system. It makes online banking reliable and much more efficient. After sending a verification link via Firebase, one gets access to the portal. Users can check eligibility criteria for active schemes, insurance, and loan capacity. It is integrated with third-party apps to trace the IP address and region of the device from which the login was attempted. Through the Microsoft Azure Face API, the face inducting the payment gets matched with all faces added by the principal user. On successful recognition, correct OTP input completes the transaction process. The principal objective of this paper will be to provide countermeasures against possible security breaches at several stages.

Research is done by Yuvaraj Duraisamy, the objective of the study **“Bringing Them Home: The Role of Azure Face API in Finding Missing Persons”** (Duraisamy et al., 2024)is to implement a system for locating missing persons with the help of the Azure Face API service. The system is realized in such a way that it can upload the image of a missing person and conduct a search in the database of known persons by comparing faces. Facial features, landmarks, and expressions are detected and analysed by the Azure Face API service to find a match. It will also allow the provision for submitting tips and information related to the cases of missing persons. The study aims to develop a tool that is effective and reliable for law enforcement agencies and for use by the public in assisting in the missing person's search.

The paper **"Face Spoofing, Age, Gender and Facial Expression Recognition Using Advance Neural Network Architecture-Based Biometric System"**(Kumar *et al.*, 2022)by Sandeep Kumar, Shilpa Rani, Arpit Jain, Chaman Verma, Maria Simona Raboaca, Zoltán Illés, and Bogdan Constantin Neagu proposes a new biometric system using advanced neural network architecture to ensure efficient face recognition. In the paper published in Sensors on 9 July 2022, the authors proposed a five-layer U-Net-based face detection and an Alex-Net-based architecture for classifying facial attributes like age, gender, and expressions with an additional module designed for addressing face spoofing. The accuracy rates achieved in the proposed model are very impressive: Spoofing- 94.17%, age - 83.26%, gender - 95.31%, and facial expression-96.9% on six benchmark datasets. This research underlines the role that soft-biometric technologies can play in increasing security while improving user interaction within different applications, especially health institutions.

This research paper**, "Head Poses and Grimaces: Challenges for Automated Face Identification Algorithms"**(Urbanova *et al.*, 2024) by Petra Urbanova, Tomas Goldmann, Dominik Cerny, and Martin Drahansky, discusses all types of problems that turn up with changes in head pose and grimaces against automated face identification algorithms. The paper is published in Science & Justice, where researchers have used a 3D face dataset with different expressions and head positions to test state-of-the-art algorithms. The results show that although small movements of the head around the frontal position slightly impact the accuracy of recognition, high deviation from it, particularly upward tilt, reduces the performance a lot.

2.3 Research Niche

Based on the research done on the Microsoft Azure Face API, password-less biometric authentication detection has never been used for securing the network while using login credentials and integrated with the PIM Just-In-Time access control to avoid unnecessary contact between each department in an organization, to avoid security breaches. Let’s research by integrating Face API with PIM using Microsoft Azure AD.

3 Research Methodology

The purpose of this research methodology is to outline the systematic approach for implementing and evaluating the project on User ID creation, biometrics integration using Face API and access control using conditional Access and Privileged Identity Management in

Microsoft Azure AD. This methodology includes the concepts of research design, data collection, data analysis, and validation processes.

Privileged Identity Management (PIM)

Some of how the risk of inappropriate, unnecessary, or excessive grants of access permissions to high-privileged resources, for example, those in Microsoft's Entra ID, Azure, and other Microsoft Online Services, such as Microsoft 365, or Microsoft Intune, can be reduced include time-based and approval-based role activation by Privileged Identity Management.

Key features

- Deliver Just Right-JIT privileged access to resources
- Create Stack Navigator Eligibility of membership or ownership of PIM for Groups
- Provide time-based access to resources by specifying allowed and denied day/time ranges
- All activate of privileged roles should be approved
- Enable MFA to active any roles
- Notifications can be obtained when privileged roles are activated
- Access reviews will do to confirm users still need roles
- Download audit history for internal or external audit

Understand PIM

The PIM concepts in this section will help you understand your organization's privileged identity requirements.

Today you can use PIM with the:(Plan a Privileged Identity Management deployment - Microsoft Entra ID Governance | Microsoft Learn)

Microsoft Entra roles – Sometimes referred to as directory roles, Microsoft Entra roles include built-in and custom roles to manage Microsoft Entra ID and other Microsoft 365 online services.

Azure roles – RBAC roles in Azure granting access to management groups, subscriptions, resource groups, and resources. Just-in-time access can be set for the Microsoft Entra security group. PIM for groups extends to Microsoft online services like Intune and Azure Key Vaults. Active group membership provisions accounts and memberships to applications via SCIM protocol.

Assign the following to these roles or groups:

Users- To get just-in-time access to Microsoft Entra roles, Azure roles, and PIM for Groups.

Groups: Any group to get Microsoft Entra and Azure roles just in time. For Microsoft Entra roles, a group should newly be created in the cloud group set as assignable to a role. For Azure roles, it can just be any Microsoft Entra ID security group. We do not recommend the assignment or nesting of a group to a PIM for Groups.

Type of assignments:

There are two types of assignments – eligible and active.

If you have made a user eligible for a role, this means he can activate the role when he needs to do privileged tasks.(*Plan a Privileged Identity Management deployment - Microsoft Entra ID Governance | Microsoft Learn*, no date; *Implementing Zero Trust with Microsoft Azure: Identity and Access Management (1 of 6) - Azure Government*, no date)

[1] Like this one: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-deployment-plan

You can now set a start and end time for every type of assignment. That brings the total to four kinds of assignments:

- Permanent Eligible
- Permanent Active
- Time-Bound Eligible, with specified dates for the start and end of the assignment
- Time-bound active, stating precisely the start and end dates of the assignment

You can renew or prolong these assignments in case they expire.

Severity has the following meaning:

- High: needs action urgently, for it is a violation of policy.
- Medium: does not need immediate action. However, it flags a possible violation of policy.
- Low: does not require immediate action. It, however, suggests a preferred policy change.

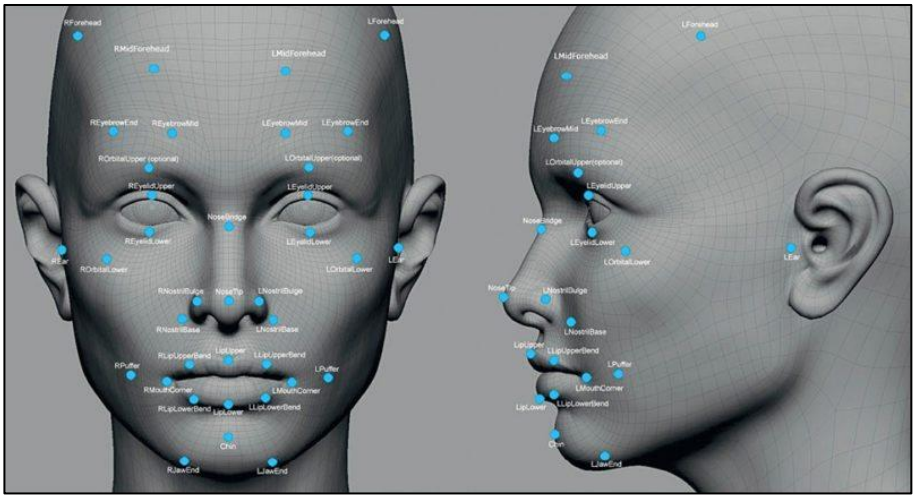

Figure 2: Microsoft Azure Cognitive Services Face API

3.1 FACE API

Biometrics:

Biometrics is the science and technology of automatically recognizing a person based on unique physical or behavioural characteristics. Several such features, including fingerprints, voice patterns, iris scans, and facial features, are peculiar to every individual; hence, biometric authentication is very close to being completely secure for identity verification. Among all biometric modalities, face recognition has become a strong niche due to its non-intrusive nature and the increasing availability of high-quality cameras in devices such as smartphones, security systems, and public surveillance networks. (What is the Azure AI Face service? - Azure AI services | Microsoft Learn)

Microsoft Azure Face API:

The Azure Face API is based on concepts of biometrics, especially facial recognition, to offer advanced face detection and analytics capabilities. Using complex algorithms, it achieves high-

level face detection and analytics such as facial feature mapping and comparing, emotion detecting, and person identifying in a database. This functionality enhances security but also allows for personalized user experiences. This Face API was launched in April 2015 by Microsoft as Project Oxford. and provided features such as face detection, verification, grouping and identification at that time.

Microsoft Cognitive Services:

In 2016, Project Oxford was rolled into Microsoft Cognitive Services,(What is the Azure AI Face service? - Azure AI services | Microsoft Learn) which manifoldly upgraded the. By 2017, the Face API was rebranded under Azure Cognitive Services, referring to its pulling into the general bundle of Microsoft AI offerings and opening more options for access and integration within the Azure ecosystem. It is also powered with detailed face detection, including finding faces within images and returning the coordinates of the face rectangle.

3.2 Implementation and Configuration of the Architecture

Design and Deployment of the Face API:

In the design and deployment of the Face API, ethical considerations were always central, especially in areas like bias and privacy. Microsoft invested in research and development to make its models fairer and more accurate for facial recognition, knowing that AI systems are biased. Face API is designed to meet rigorous data privacy regulations, such as the GDPR, with stringent privacy controls in place for protecting user data.(What is the Azure AI Face service? - Azure AI services | Microsoft Learn; Azure identity & access security best practices | Microsoft Learn)

Today, the Azure Face API remains one of the integral parts of Azure Cognitive Services and becomes ever more important in answering the increasing demand for reliable and ethical face recognition solutions. Its development reflects the broader commitment by Microsoft to the provision of cutting-edge AI technologies while addressing the ethical challenges they present.

Conditional Access and Policies:

Conditional Access and Policies lie at the heart of modern security frameworks, especially when advanced biometric systems such as Azure Face API are being integrated. In essence, Conditional Access is an Azure AD feature that will enforce certain controls on how users access corporate resources based on certain specified conditions. This approach improves security by ensuring access to sensitive data, applications, and services only to authorized persons under certain circumstances that reduce possible risks.(Implementing Zero Trust with Microsoft Azure: Identity and Access Management (1 of 6) - Azure Government; Azure identity & access security best practices | Microsoft Learn)

Benefits of Using Conditional Access with Policies:

Security Enhanced process: This means that the risk of unauthorized access will decrease if conditional access is combined with biometric authentication.

Compliance: By implementing Conditional Access policies that involve biometric authentication, the chances of compliance with different regulatory provisions regarding protection and access to data by organizations will be improved.

[2] Like this one: https://learn.microsoft.com/en-gb/azure/ai-services/computer-vision/overview-identity#face-detection-and-analysis

Flexibility: Conditional Access Policies can be fine-tuned to specific security requirements while trying not to sacrifice usability. which allows an organization to adapt to various scenarios.
User Experience: Compared to traditional passwords or security tokens, Biometric authentication has made for a frictionless and seamless user experience.

4 Design Specification

This design specification document describes the technical and functional requirements for the implementation of user ID creation, biometrics integration using the Face API, and access control using Conditional Access and Privileged Identity Management (PIM) in Microsoft Azure AD. This document provides a detailed description of the system architecture, components, and processes to ensure a successful evaluation of the tasks performed.

Microsoft 365 Admin Centre:
The cloud-based management platform for your business is Microsoft 365 Admin Centre. the fulfilment of duties such as user additions and deletions, license changes, and password resets. More precise control is possible with specialised workspaces like those for device management or security.

Microsoft Azure Portal:
The Azure portal is a single, web-based console that allows you to build and administer every Azure resource. May create, oversee, and keep an eye on anything on the portal, from straightforward web apps to intricate cloud projects. The PIM (JIT) feature is one of the premium features in the Azure cloud platform under identity governance and Face API authentication.

Microsoft Entra Admin Centre:
The Microsoft Entra admin centre is a web-based identity portal for Microsoft Entra products. Employees, devices, enterprise apps, and resources may all be kept safe with their identity, authentication, policy, and protection features.

Microsoft Intune Admin Centre:
Microsoft Intune is a cloud-based endpoint management tool. It provides user access to organisational resources and facilitates app and device administration across many platforms, such as mobile phones, desktop PCs, and virtual endpoints.

4.1 Objective:

Secure and maintain user identity plans and regulate the access control towards a regulated industry using Azure AD, Face API, Conditional Access policies, and Privileged Identity Management (PIM).

4. 2 Functional Requirements

4. 2. 1 User Identity Creation and Administration

Include the ability to create a new user ID with the correct licenses and roles for the facility. The details of the user shall be captured as described here and stored. Make the Admin side more user-friendly when it comes to handling the User IDs.

4. 2. 2 Biometric Authentication Integration

Another scenario in its application is its use in second-factor authentication via Azure Face API. When using Face API, it is crucial to ensure proper integration with Azure AD users; and put measures in place that can be used in case face recognition fails.

4. 2. 3 Conditional Access Policies

Create and apply Conditional Access policies, where specific users are to perform biometric identification. Ensure that the policies should be made far from rigid regarding the roles of the users and the compliances. Record and watch real-time access control events.

4. 2. 4 Privileged Identity Management(Plan a Privileged Identity Management deployment - Microsoft Entra ID Governance | Microsoft Learn)

Ensure that PIM is used for the management and reviews of roles that provide privileged access. Offer the rights to the admins for generating, assigning, and auditing of role assignments. Support the possibility of the automatic check of access and assignments of the roles according to their defined parameters.

4. 3 Component Interaction

- User Management Interface: It provides the ability to make and unmake the user IDs using an Admin.
- Azure AD: Control centre which can be used to control the users.
- Face API: Biometric authentication services provider.
- Conditional Access Policies: Access should follow authorization based on a set number of permissions given by an admin.
- PIM: This reviews access and manages roles of privileged access.

5 Implementation

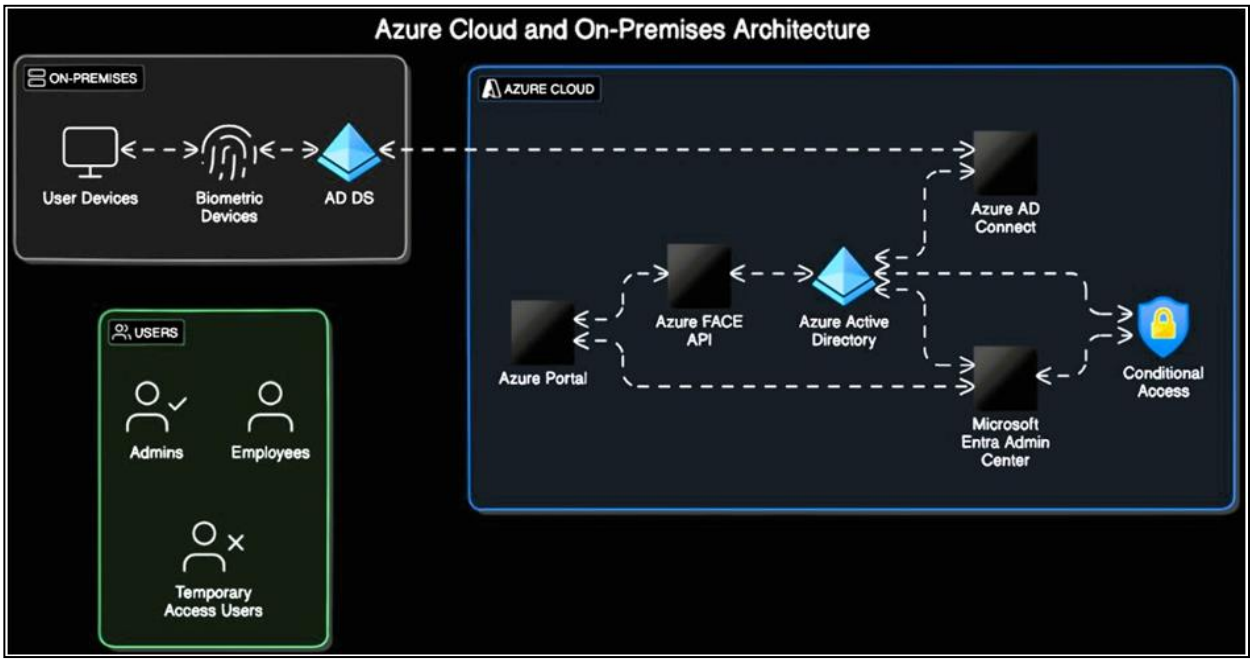

Figure 3: Proposed Architecture Diagram for Face API and PIM(JIT) Access control

The architecture diagram illustrates creating and setting up User IDs within the Microsoft 365 Admin Console. First, run Microsoft 365 Admin Console and log in. Add a new user. From

the left menu, click "Users," then "Active users," and finally "Add a user." Under "User details," fill in all the relevant details of the user, such as the name of the user and the username, assigning the appropriate license before clicking "Add" to create the user ID.

First, buy the Face API by logging into Azure Marketplace, searching for "Face API", and subscribing. Next, sync Face API with the Azure AD users by creating a "Face API" account on the Azure portal and then linking it with Azure AD for two-step verification.

To set up a Conditional Access policy that requires facial biometrics for certain users, sign in to Azure AD and go to "Azure Active Directory" in the Azure portal. From there, select "Security" and then "Conditional Access." Click "New policy" and then provide a name for this policy. Under "Assignments," select those users or groups to which this policy will apply. Under "Cloud apps or actions," select which applications will require this policy. Under "Conditions," configure device and location settings. In "Access controls," select "Grant" and then require "Face API authentication." By reviewing the details and saving and enabling the policy.

Setting up a role-based access review with Microsoft Entra requires logging in to Microsoft Entra with an administrator account, then connecting to the module of Identity Governance by selecting "Identity Governance" and afterwards "Privileged Identity Management," and selecting either "Microsoft Enterprise roles" or "Azure resources." Select "Access Reviews" under "Manage," then "New" to create a new access review. Set up a new access review. Configure the new access review. Add assignments by selecting the proper role and member, setting the type of assignment (Eligible or Active), and duration. Click "Assign" to complete the assignment of the role.

To Approve the Requests for the Role Activation in Microsoft Entra

- Log in using Global Administrator credentials in the Microsoft Entra Admin Center.
- Click on "Identity Governance"
- Click on "Privileged Identity Management"
- Click on "Approve requests"

Now you can view all pending requests and approve or reject them accordingly.

In the "Identity Governance" section of Azure Portal, users can create resources and request departmental access using "Add a resource" feature. After setting up access approval in settings, access is in place through "My event" tab in Outlook with approval or rejection notifications sent to IT Department Head. Requests to extend expiring role assignments should be submitted through the PIM portal "My Roles" section no later than 14 days prior to its expiration. The process for extensions is prompted by end-users.

5.1 User ID Creation and Setup

Objective: Create and set up Microsoft 365 Admin Console's user IDs

5.1.1 Login to Microsoft 365 Admin Console:

- Open Microsoft 365 Admin Console.
- Login to the Microsoft 365 Admin Console.

5.1.2 Add User:

- On the left side menu, select "Users."

- Then "Active users."
- Hit "Add a user."

5.1.3 Fill User Details:

- In the "User Details" area, finish the required details such as name, username etc.,
- Assign the user the proper license.
- Hit the "Add" button to create the User ID.

5.2 Biometrics Concept

Objective: Set up biometric authentication by using Face API.(What is the Azure AI Face service? - Azure AI services | Microsoft Learn)

5.2.1 Purchase Face API:

- Locate the search bar and type "Face API".
- Subscribe to the same and purchase the subscription.

5.2.2 Sync Face API with Azure AD Users:

- Create a "Face API" account on the Azure portal.
- Next let us associate Face API with Azure AD for two-step verification.

5.3 Create a New Policy for Conditional Access

Objective: To implement a Conditional Access policy that would ask for face biometrics of a few selected users. (Azure identity & access security best practices | Microsoft Learn; Implementing Zero Trust with Microsoft Azure: Identity and Access Management (1 of 6) - Azure Government)

5.3.1 Login to Azure AD:

- Go to the Azure portal and log in with your Admin account.

5.3.2 Create Conditional Access Policy:

- Go to "Azure Active Directory."
- Click on "Security" > "Conditional Access."
- Click "Create policy."

5.3.3 Configure Policy:

- Name the policy.
- In "Assignments," specify the users or groups the policy applies to.
- In "Cloud apps or actions," specify applications needed for this policy.
- In "Conditions," go to device and location conditions.
- In "Access controls," select "Grant" and make "Face API authentication" required.

5.3.4 Save and Enable Policy:

- Review details.
- Click "Create" to save.
- Either enable the policy and, if there are users, ensure this is done.

5.4 Create Access Reviews

Objective: Set up role-based access review using Microsoft Enterprise.

5.4.1 Sign in to Microsoft Entra Admin Center:

- Login In by the user with the identified roles.

5.4.2 Navigate to Identity Governance:

- Click on "Identity Governance" > "Privileged Identity Management.
- Select "Microsoft Enterprise roles" or "Azure resources."

5.4.3 Create New Access Review:

- Click "Access Reviews" under "Manage."
- Click "New" to create a new access review.
- Create a New Access Review with configuration settings.

5.4.4 Add Assignments:

- Click "Add Assignments."
- Choose the role and member for the assignment.
- Configure assignment type (Eligible or Active) and duration.
- Click "Assign" to finalize the role assignment.

5.5 Pending Request Approval

Objective: Approve role activation requests in Microsoft Entra.

5.5.1 Sign in to Microsoft Entra Admin Center:

- Sign in with Global Administrator credentials.

5.5.2 Approve Requests:

- Navigate to "Identity Governance" > "Privileged Identity Management" > "Approve requests."
- Review and approve or deny pending requests.

5.6 Creating Resources and Department Access Requests

Objective: Create available resources for departments and address access requests.

5.6.1 Create Resources:

- Area in the Azure portal named "Identity Governance."
- Implement. The "Add a resource" creates departments and configures requisite access approvals.

5.6.2 Department Access Request:

- Departmental access is allowed as users request through the "My event" tab displayed on the Outlook app.
- The IT Department Head gets mail for the request to be approved or disapproved.
- Notifies through mail whether it is affirmed or disaffirmed.

5.7 Extend Role Assignment

Objective: Exposed users to extend expiring role assignments.

5.8 Role Extension:

- Users may submit an extension from their "My Roles" in the Privileged Identity Management portal.
- Extensions are requested on expiring roles, at least, 14 days.
- End users will be walked through the process and take necessary action for requesting and finalizing extensions.

5.8.1 Complete access reviews

Objective: Note Steps in this section might vary slightly depending on where you begins the portal. Sign in to the portal as a user who is assigned to one of the below roles.

- Browse to Essential Identity Governance > Privileged Identity Management
- For Microsoft Sign-in roles: Select Microsoft Sign-in roles.
- For Azure resources: Select Azure resources
- Choose the access review you want to work with. (Plan a Privileged Identity Management deployment - Microsoft Entra ID Governance | Microsoft Learn; What is Just-in-Time Access (JIT)?)

5.8.2 Stop an access review

All-access reviews have a due date; however, the reviewer can stop them if the review is "active". You cannot stop and start a review again.
After the review instance is activated, and there has been at least one decision made by reviewers on it, the entire access review can be reset by clicking the "Reset" button to discard all decisions made on it. When an In-Progress access review is reset, all users are marked as Not Reviewed again.

5.8.3 Applying for an Access Review

After an access review is completed, either reached its end date or the manual process has stopped, the Apply button will take access away from denied users into a role. This step is where access to a person's role assignment is removed if access to that person was denied during the review. If Auto Apply was configured when the review was created, this button would always be disabled, as the review would be applied automatically rather than manually.

5.8.4 Delete an access review

If you do not desire the review, to take place any longer then you can simply delete the review. To delete the access review from the service of Privileged Identity Management click on Delete.

6 Evaluation

6.1 Plan testing

Create test users to verify PIM settings work as expected before you impact real users and potentially disrupt their access to apps and resources. Build a test plan to have a comparison between the expected results and the actual results.

The following table shows an example test case:

Role	Expected behaviour during activation	Actual results
Global Administrator	• Require MFA • Require approval • Require Conditional Access context (Public preview) • Approver receives notification and can approve • Role expires after the pre-set time	Pass Pass Pass Pass Pass
Users	• Request JIT permission • Requested JIT permission to extend • Request Resource permission • Requested Resource permission to extend • Scheduling Meetings or new Events using Calendar • FACE API Authentication	Pass Pass Pass Pass Pass Deny

6.2 Results

Beyond that, the execution of creating user credentials and getting linked with the Microsoft Azure Face API by using the resources available in the Azure platform the integrating between the user's database and PIM JIT concept gets corrupted due to the subscription license issue, on contacting the Microsoft support team as per the expert suggestion the license can be provided only for the authorized domain linked with Microsoft products. Since it was a free trial, this particular action cannot be performed by this end. The alternative solutions of SDK, VMs, and Powershell have been tried and executed but the same output was executed. However, only by the appropriate subscription of FACE API, this function can fully succeed. However, the positive approach of this research is that if an organization has connected within the Microsoft privileged products this action can be performed and executed successfully. And the tasks created after successful authentication by using PIM JIT access control can be performed flawlessly. The results stated that the integration of Face API and PIM in Azure AD for reducing the risk of data breaches can be performed by having the proper subscription and the organization can enhance their security by using this methodology.

6.3 Discussion

The literature review explored the use of Face API and JIT PIM access control but not specifically for integrating both in login credentials. Early studies focused on improving limited

security features, like identifying missing persons and groups, but only partially achieved PIM management in Azure Face API. Contributions to the RBAC JIT domain highlight the potential of biometric-based passwordless authentication as highly secure. The protection of sensitive biometric data and the gaining of trust by users become very important with AI increasingly being used in cyberattacks. The increasing use of biometric authentication marks the trend of evolved IT security measures despite these challenges. Using PIM, state-of-the-art biometric technology, among others, ranks Microsoft Azure Active Directory as one of the access management services to the cream.

7 Conclusion and Future Work

To conclude, a strong and secure user authentication system was designed using Azure Active Directory along with the biometric feature supported by the Azure FACE API. This architecture is targeted at achieving a more secure, stress-reduced process by using biometric data as a second step to guarantee that resources make it to the right user in the competitive market. The addition of Conditional Access policies delivers another layer of security that eases dynamic control of who can access the system under set conditions based on several things like user roles, locations, and devices. In addition, the capability to perform role assignments and access reviews within the Microsoft Entra Admin Center allows for very fine-grain control and periodic auditing of user privileges, thereby continually ensuring that access rights are aligned with organizational policies.

In the future, if Microsoft Azure AD grants full manageable access to passwordless authentication such as Facial recognition to the organization of regulated industries healthcare, finance and government then the authentication system will be much more safe and secure to avoid multiple logins and unauthorized access for the users by enabling JIT access control. This can enhance the security of the user interface and domain specification.

References

Azure identity & access security best practices | Microsoft Learn (no date). Available at: https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices (Accessed: 11 August 2024).

Carver, J.C. *et al.* (2020) 'Conference Highlights: JIT Fault Prevention, Motivated Modeling, Security in Requirements, and Improving Team Performance', *IEEE Software*, 37(4), pp. 83–86. Available at: https://doi.org/10.1109/MS.2020.2986840.

CyberArk Expands Just-in-Time Capabilities Across Industry's Broadest Privileged Access Management Portfolio - EBSCO (no date). Available at: https://research.ebsco.com/c/x47ol5/viewer/html/qugzsul62b (Accessed: 11 August 2024).

Ducasse, Q., Cotret, P. and Lagadec, L. (2023) 'JIT Compiler Security through Low-Cost RISC-V Extension', *2023 IEEE International Parallel and Distributed Processing Symposium Workshops, IPDPSW 2023*, pp. 125–128. Available at: https://doi.org/10.1109/IPDPSW59300.2023.00032.

Duraisamy, Y. *et al.* (2024) 'Bringing Them Home: The Role of Azure Face API in Finding Missing Person', *Proceedings - 2024 5th International Conference on Mobile Computing and*

Sustainable Informatics, ICMCSI 2024, pp. 71–76. Available at: https://doi.org/10.1109/ICMCSI61536.2024.00017.

Identity Attack Vectors: Strategically Designing and Implementing Identity Security, Second Edition (no date). Available at: https://learning.oreilly.com/library/view/identity-attack-vectors/9798868802331/?ar= (Accessed: 11 August 2024).

Implementing Zero Trust with Microsoft Azure: Identity and Access Management (1 of 6) - Azure Government (no date). Available at: https://devblogs.microsoft.com/azuregov/implementing-zero-trust-with-microsoft-azure-identity-and-access-management-1-of-6/ (Accessed: 11 August 2024).

Jaouhari, S. El, Bouabdallah, A. and Bonnin, J.M. (2018) 'A secure WebRTC/WoT-based health-care architecture enhanced with access control', *International Conference on Information Networking*, 2018-January, pp. 182–187. Available at: https://doi.org/10.1109/ICOIN.2018.8343107.

Kumar, S. *et al.* (2022) 'Face Spoofing, Age, Gender and Facial Expression Recognition Using Advance Neural Network Architecture-Based Biometric System.', *Sensors (Basel, Switzerland)*, 22(14). Available at: https://doi.org/10.3390/S22145160.

Liqing, L. *et al.* (2011) 'Research of extended RBAC model on permission control in WEB information system', *2011 IEEE 3rd International Conference on Communication Software and Networks, ICCSN 2011*, pp. 359–362. Available at: https://doi.org/10.1109/ICCSN.2011.6014584.

Plan a Privileged Identity Management deployment - Microsoft Entra ID Governance | Microsoft Learn (no date). Available at: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-deployment-plan (Accessed: 11 August 2024).

Satish Babu, B. V. *et al.* (2024) 'Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments', *2024 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing, INCOS 2024 - Proceedings* [Preprint]. Available at: https://doi.org/10.1109/INCOS59338.2024.10527499.

Sharma, K. *et al.* (2022) 'Advanced Bank Security and Management System', *2022 IEEE 7th International conference for Convergence in Technology, I2CT 2022* [Preprint]. Available at: https://doi.org/10.1109/I2CT54291.2022.9825468.

Urbanova, P. *et al.* (2024) 'Head poses and grimaces: Challenges for automated face identification algorithms?', *Science & Justice*, 64(4), pp. 421–442. Available at: https://doi.org/10.1016/J.SCIJUS.2024.06.002.

What is Just-in-Time Access (JIT)? (no date). Available at: https://delinea.com/what-is/just-in-time-access (Accessed: 11 August 2024).

What is the Azure AI Face service? - Azure AI services | Microsoft Learn (no date). Available at: https://learn.microsoft.com/en-us/azure/ai-services/computer-vision/overview-identity (Accessed: 11 August 2024).