**3.5 GenAI-Powered Unified Authentication and Authorization (A&A) System for Multi-Cloud Environments**

**Problem Statement:**

As organizations increasingly adopt multi-cloud strategies, ensuring secure and seamless access to applications and data across cloud platforms like **Microsoft Entra (Azure AD)**, **AWS IAM**, and **Google Cloud IAM** is critical. The challenge lies in creating a **GenAI-enhanced unified Authentication and Authorization (A&A) system** that can streamline authentication processes while leveraging AI for intelligent access management and real-time decision-making.

This system must ensure secure access across multiple cloud environments, provide **Role-Based Access Control (RBAC)**, and employ **GenAI models** to continuously analyze and optimize user access based on risk profiles, behavior patterns, and dynamic needs. It should enhance the security and performance of the A&A process by providing AI-powered insights and predictions to better manage access privileges across platforms.

**Objective:**

Build a **GenAI-powered Authentication and Authorization system** that:

1. **Seamlessly integrates** with **Microsoft Entra (Azure AD)**, **AWS IAM**, and **Google Cloud IAM** for centralized and secure authentication.
2. Implements **GenAI models** to dynamically analyze user access behavior and predict potential security risks, offering **real-time access management** insights.
3. Provides **Role-Based Access Control (RBAC)** for both end-users and administrators, ensuring intelligent access management based on evolving user needs and behaviors.
4. Ensures secure and compliant multi-cloud access management, enhancing decision-making through AI-driven insights and predictions.
5. Includes a **unified admin dashboard** powered by GenAI to monitor access activities, predict anomalies, and make real-time recommendations for access controls.

**Design Strategy and Approach:**

1. **Unified GenAI-Enhanced Authentication**:
   * Implement **OAuth2.0**, **OIDC**, and **SAML** to securely authenticate users across cloud platforms.
   * Use **GenAI models** to analyze user access patterns and make recommendations on access levels based on predicted risk.
2. **AI-Powered Role-Based Access Control (RBAC)**:
   * Integrate AI models to assess the risk associated with access roles and dynamically adjust user privileges based on predicted behaviors and organizational policies.
3. **GenAI-Driven Predictions**:
   * Use GenAI models to forecast potential access risks, predict anomalous behavior, and recommend security actions in real-time, such as access restrictions or role adjustments.
4. **Admin Dashboard with AI Insights**:
   * Build a **centralized admin dashboard** where AI-driven insights about user behavior, predicted risks, and access control recommendations can be viewed and acted upon.

**Technologies to Be Used:**

* **Python**: Backend for implementing AI models, authentication logic, and cloud integration.
* **GenAI models**: For predicting access risks and making access control recommendations.
* **Microsoft Entra (Azure AD)**, **AWS IAM**, **Google Cloud IAM**: For multi-cloud authentication and authorization.
* **Angular**: For developing the unified AI-enhanced admin dashboard.
* **RESTful APIs**: For communication between the A&A system, GenAI models, and cloud platforms.
* **Key cloak / Octa**

**Testing Requirements:**

* **Unit Testing**: For AI models predicting risk and access recommendations.
* **Integration Testing**: Ensure seamless communication between cloud authentication services and AI models.
* **Performance Testing**: Simulate high-volume user access to test AI’s real-time decision-making and risk predictions.
* **UI Testing**: Ensure that the AI-powered admin dashboard provides actionable insights in real-time.

**Documentation Requirements:**

* **API documentation** explaining how GenAI models integrate with multi-cloud platforms.
* **User Guide** for administrators on using AI insights for managing roles and permissions.
* **Design document** outlining the architecture of the unified GenAI-enhanced A&A system.

**Time Frame:**

**2 weeks**, in-person development by a **POD of 3 individuals** at **Centific premises**.