Project Design Phase

Solution Architecture

Date	2-10-2025
Team ID	NM2025TMID07413
Project Name	Optimizing User, Group, and Role Management with Access Control and Workflows
Marks	4 Marks

Solution Architecture: Optimizing User, Group, and Role Management with Access Control and Workflows

1. Overview

The solution is built around a centralized identity and access management system that connects all users, applications, and approval workflows. It ensures that the right people get the right level of access at the right time through automation, policies, and secure workflows

2. Key Components

Identity Store:

The main database that holds all user information (e.g., Active Directory, Azure AD, or Okta).

User, Group, and Role Management Service:

Handles creating, updating, and deleting users, groups, and roles. It defines role hierarchies and links roles with permissions.

Access Control Engine:

Uses Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) to decide who can access what.

Workflow Engine:

Automates access requests, approval processes, and periodic reviews.

Provisioning Layer:

Automatically grants or removes access in connected systems once approval is completed.

Self-Service Portal:

Lets users request access and view the status of their permissions.

Audit and Compliance Module:

Tracks every action for security audits and compliance reporting.

Integration Layer:

Connects with HR systems, IT helpdesks, and cloud applications for smooth data flow.

3. Workflow Process

1. A user submits an access request through the self-service portal.

2. The workflow engine triggers an approval process based on predefined rules.

3. The approver reviews and approves or denies the request.

4. Once approved, the provisioning layer automatically grants access.

5. The audit module logs all actions for future review.

6. Periodic review workflows verify that access rights are still valid.

4. Security and Compliance Features

Enforces least privilege access (only what’s needed).

Automates access reviews and role certifications.

Provides full audit trails for every action.

Detects and prevents conflicts of interest (SoD violations).

Ensures encryption and multi-factor authentication (MFA) for critical roles.

5. Benefits

Streamlined and automated user access management.

Reduced manual errors and administrative workload.

Stronger data security and regulatory compliance.

Faster onboarding and de-provisioning.

Centralized visibility and control over all user permissions.

6. Technology Stack (Example)

Identity Store: Active Directory / Azure AD / Okta

Workflow Engine: Camunda / Temporal / Power Automate

Access Control Engine: Open Policy Agent (OPA) / Custom RBAC module

Database: PostgreSQL / MySQL

Audit & Logs: Elasticsearch / Splunk

Frontend: React / Angular (for Admin & User Portals)

APIs: REST / SCIM / GraphQL

7. Summary

This architecture centralizes identity data, defines clear roles and access policies, automates

approval workflows, and enforces strict security controls. It makes user and role management faster, safer, and fully auditable — improving both productivity and compliance.

Solution Architecture Description:

The proposed solution architecture for optimizing user, group, and role management with access control and workflows is designed to provide a centralized, secure, and automated system for handling user identities and permissions.

This architecture integrates various modules that work together to manage user accounts, define access roles, control permissions, and automate approval processes. The main goal is to ensure that users receive appropriate access based on their roles while maintaining strong security, compliance, and operational efficiency.

At the core of the architecture lies an Identity Management System, which serves as the central repository for all user and group data. It is connected to an Access Control Engine, which applies either Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) policies to determine who can access specific resources.

A Workflow Automation Engine manages the request, approval, and provisioning processes for user access. This ensures that access changes follow a consistent and auditable path, reducing manual intervention and administrative workload.

The Provisioning Layer automatically updates user permissions across different systems and applications once approval is granted. All activities are recorded in an Audit and Compliance Module, which tracks user actions and provides reports for governance and security reviews.

The architecture also includes a Self-Service Portal for users to request access and view their current permissions, as well as an Admin Console for system administrators to monitor, approve, and manage roles.

Integration with external systems such as HR databases, cloud applications, and authentication providers (e.g., Active Directory, Azure AD, or Okta) ensures smooth data synchronization and unified access management.

This architecture promotes efficiency, scalability, and security by automating repetitive tasks, enforcing policy-based access, and maintaining transparency through continuous monitoring and audits. It helps organizations reduce risks, improve compliance, and deliver a seamless experience for both administrators and end users.

Example: Optimizing User, Group, and Role Management with Access Control and Workflows

Scenario:

A university’s IT department manages thousands of students, faculty, and administrative staff who need access to different systems such as the learning portal, library system, HR platform, and exam management tool.

Before optimization, all access requests were handled manually by the IT team through emails, which caused delays, errors, and security risks.

Problem:

Manual access approval took 2–3 days per request.

Users often had unnecessary access (e.g., old staff accounts not removed).

No clear tracking of who approved what access.

High workload for the IT administrators.

Solution Implementation:

The university implemented a centralized identity and access management system using Role-Based Access Control (RBAC) with automated workflows.

1. User Management:

All student and staff details are automatically imported from the HR and student enrollment systems.

2. Group Management:

Users are grouped automatically (e.g., “Students”, “Faculty”, “Admin Staff”) based on department and role.

3. Role Management:

Each role has defined permissions — for example:

Student → Access to learning portal and library system

Faculty → Access to exam management and course creation tools

Admin Staff → Access to HR and finance applications

4. Access Control:

The RBAC engine ensures users get only the permissions assigned to their roles. If someone changes departments, access is automatically updated.

5. Workflow Automation:

When a user requests extra access (e.g., research database), the request is sent automatically to the department head for approval.

Once approved, the system provisions access instantly without IT intervention.

All approvals and actions are logged for audits.

Outcome:

Access request time reduced from 3 days to a few minutes.

IT team workload dropped by 40%.

No more unauthorized or outdated access.

Full audit trail available for compliance checks.

Conclusion:

Through centralized management, defined roles, and workflow automation, the university achieved secure, efficient, and transparent access control — ensuring the right people have the right access at the right time.