Project Design Phase
Solution Architecture

Date	2 NOVEMBER 2025
Team ID	NM2025TMID04605
Project Name	Optimizing User, Group and Role Management with Access Control and Workflows
Marks	4 marks

Solution Architecture:

Goals of the Architecture:

- Automate user, group, and role management processes.
- Ensure secure and policy-based access control through RBAC.
- Enable workflow-driven approval and modification of user permissions.
- Maintain centralized tracking and audit logs for every user action.
- Reduce manual workload and improve system scalability.

Key Components:

- **User Table**: Stores user details, roles, and associated permissions.
- **Group Table:** Maintains information about departments or teams and their assigned roles.
- **Role Table:** Defines the access rights and privileges for each role.
- **Access Control Module:** Implements RBAC (Role-Based Access Control) logic to manage user privileges.
- **Workflow Engine:** Automates approval, review, and deactivation processes for user access requests.

Development Phases:

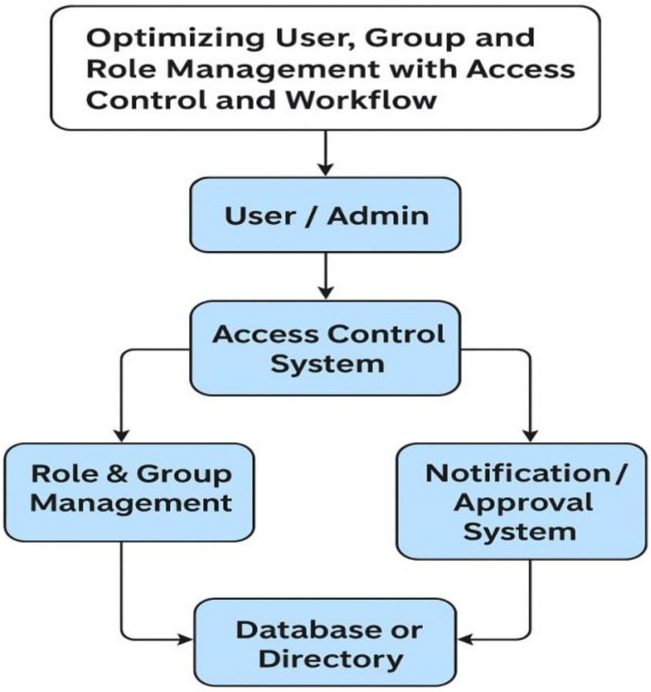
1. **Requirement Analysis:** Identify existing gaps in user and role management.
2. **Design Access Policies**: Define roles, permissions, and group-level privileges.
3. **Workflow Implementation**: Create automated approval workflows for access requests.
4. **Integration & Testing:** Link the RBAC system with workflow automation and validate through test cases.
5. **Monitoring & Feedback**: Continuously monitor logs, collect admin feedback, and refine policies for better performance.

⊗ **Solution Architecture Description**:

The solution architecture is designed to provide a secure and automated framework for managing users, groups, and roles within an organization. It leverages Role-Based Access Control (RBAC) principles integrated with a workflow automation engine to ensure that all access-related activities follow predefined rules and approval chains. When a user requests access to a resource or role modification, the workflow system automatically routes the request to the appropriate approver. Once approved, the user is granted access based on the assigned role. The system also handles user deactivation through automated triggers when employees leave or roles change.

This architecture enhances data integrity, security compliance, and operational efficiency while reducing the dependency on manual administration. With centralized monitoring and audit trails, organizations can ensure accountability, faster response times, and complete visibility into access control operations.

Example - Solution Architecture Diagram:


Optimizing User, Group and Role Management with Access Control and Workflow
User / Admin
Access Control System
Role & Group Management
Notification / Approval System
Database or Directory

Solution Architecture