Project Design Phase-II

Technology Stack (Architecture & Stack)

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

Technical Architecture (Summary)

The system uses a layered architecture with automation, security, and centralized control at its core.

User Interface Layer: Provides admin dashboards, self-service portals, and approval screens for managing users and roles.

Application Layer: Contains the workflow engine for onboarding, offboarding, and access approvals,

and an RBAC (Role-Based Access Control) module to manage permissions.

Integration Layer: Connects with HR systems, identity providers (like Azure AD or Google Workspace), and cloud applications for synchronization.

Data Layer: Stores user profiles, roles, group details, and audit logs securely in a centralized database.

Security Layer: Handles authentication, authorization, MFA, and continuous monitoring for access activities.

Data Flow Example:

When HR adds a new employee, the workflow engine automatically creates a user account, assigns a role via RBAC, and logs all actions in the

audit system. Similarly, offboarding and access requests follow automated, approval-based workflows to maintain security and compliance.

Table-1 : Components and Technologies:

S.No	Component	Description	Technology Used
1	User Interface	Provides dashboards for admins and users to manage access and approvals.	React.js / Angular
2	Authentication & Authorization	Ensures secure login and role-based access control (RBAC).	Keycloak / Azure AD / OAuth 2.0
3	Workflow Engine	Automates onboarding, offboarding, and approval processes.	Camunda / Temporal
4	Integration Layer	Connects HR systems and third-party applications for user data sync.	RESTful APIs / SCIM

5	Database	Stores user accounts, roles, groups, and activity logs.	PostgreSQL / MySQL
6	Audit & Compliance Module	Tracks and logs user actions for reporting and compliance.	ELK Stack (Elasticsearch, Logstash, Kibana)
7	Notification System	Sends alerts and approval notifications to users and managers.	Email / Push Notification Service
8	Deployment & Monitoring	Ensures scalable and reliable deployment with performance tracking.	Docker / Kubernetes / Grafana

Summary:

This table model highlights how each component works together — from user access management and workflow automation to security, integration, and monitoring — to create a complete, optimized access control system.

Table-2 : Applications and Characteristics:

S.No	Application Area	Description	Key Characteristics
1	Enterprise Access Management	Controls employee access to internal systems and data.	Secure, centralized, and role-based.
2	Educational Institutions	Manages student, teacher, and admin access to digital platforms.	Multi-level roles, easy onboarding, audit tracking.
3	Healthcare Systems	Ensures secure access to patient records and medical data.	High data privacy, compliance-driven, access logging.
4	E-commerce Platforms	Manages vendor, customer, and admin roles efficiently.	Scalable, user-friendly, real-time updates.
5	Government Portals	Provides controlled access for citizens and officials.	Transparent, compliant, and workflow-based approvals.

6 Food Delivery Apps Controls roles for customers, delivery agents, and restaurant owners. Fast role switching, automated approvals, secure login.

Summary:

This system can be applied across multiple industries with key characteristics like security, scalability, automation, and compliance, ensuring smooth user and role management.