IDEATION PHASE

BRAINSTORM & IDEA PRIORITIZATION

TEMPLATE

Date	1 November 2025
Team ID	NM2025TMID07110
Project Name	Optimising user,group, and role management with access control and workflows
Maximum Marks	4 marks

Adaptive Access Management using Behavioral Analytics

In traditional access control systems, users are assigned fixed roles and permissions based on predefined policies. However, this static approach often fails to detect unusual or unauthorized access patterns that occur due to compromised credentials or insider threats.

Adaptive Access Management using Behavioral Analytics introduces dynamic and intelligent access control. The system continuously monitors user behavior — such as login patterns, device usage, access frequency, and location — to detect anomalies.

If the behavior deviates from the norm (e.g., a user logging in from an unfamiliar device or accessing sensitive data at odd hours), the system can automatically adjust permissions, trigger multi-factor authentication, or temporarily restrict access.

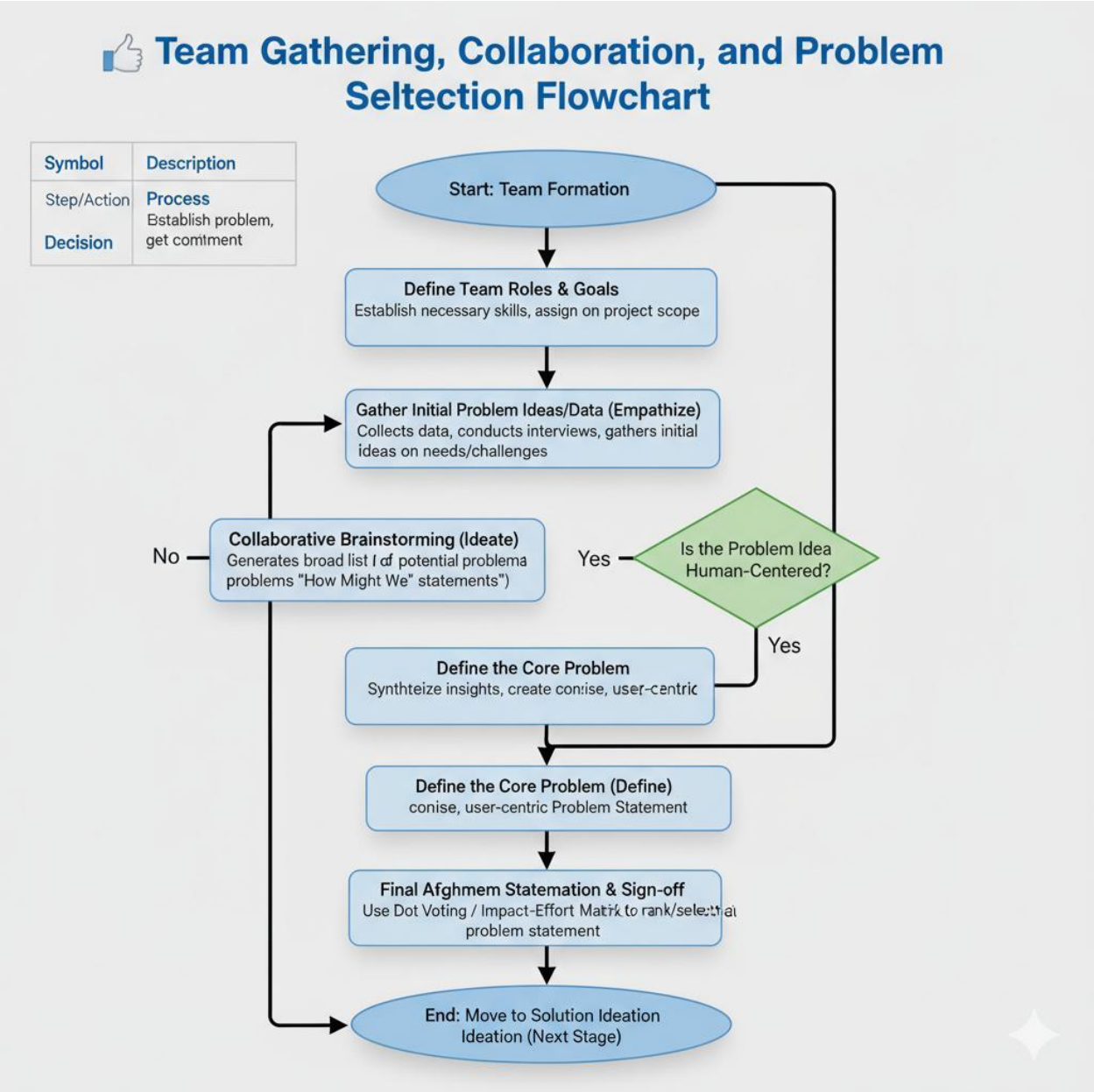
This approach combines

- Machine Learning Models to establish normal behavioral baselines.
- Context-Aware Access Control that adapts in real time.
- Workflow Automation for access review and anomaly response.

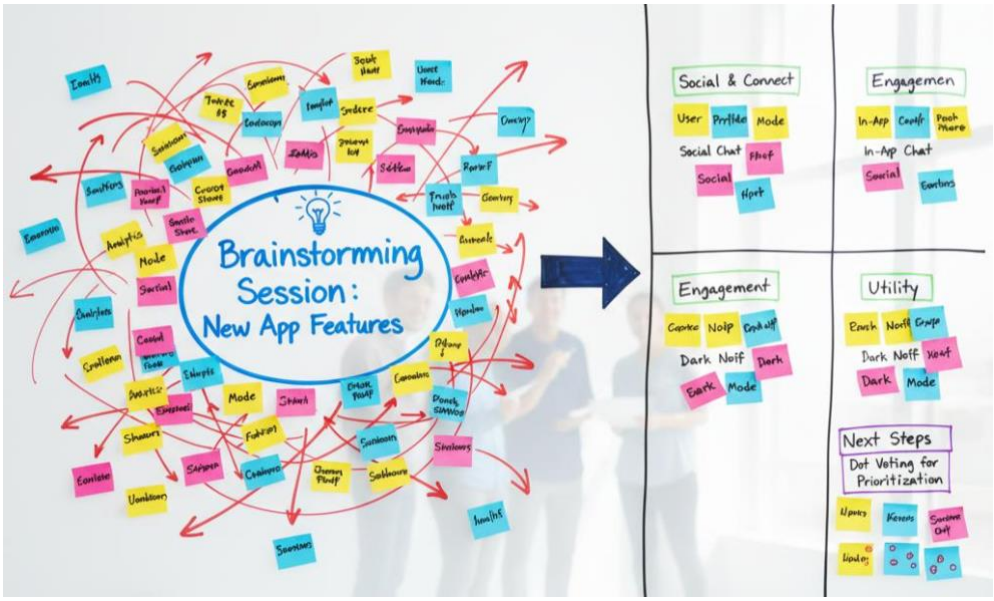
Ideation Goal:

To design a smart, self-adjusting access control system that enhances security, reduces administrative burden, and improves compliance in dynamic organizational environments.

Step 1: Team Gathering, Collaboration and Select the Problem Statement



Step 2: Brainstorm, Idea Listing and Grouping



Step-3: Idea Prioritization:

This is the most critical factor in an Identity and Access Management (IAM) contex

- Risk Reduction: Does the idea eliminate a known security vulnerability (e.g., revoking access instantly upon termination) or enforce a necessary security principle
- High Priority Example: Implementing Multi-Factor Authentication (MFA) for all administrator roles or enforcing the Principle of Least Privilege (PoLP) by reviewing and tightening existing roles.

Compliance Mandates: Is the idea required to meet regulatory standards (e.g., GDPR, HIPAA, SOX)? Features necessary for audit logging and reporting fall into this category.

High Priority Example: A new workflow for periodic access review/recertification to prove compliance to auditors.

- Operational Efficiency and Cost Reduction (Should-Haves)

This measures how much time, effort, or money the idea saves the IT and administrative teams.

- Automation Potential: Does the idea automate a high-volume, manual, and error-prone task? Manual management of user access is a key source of security risks and inefficiency.
- High Priority Example: Automating user provisioning and deprovisioning based on HR system changes (e.g., automatically creating accounts on onboarding and disabling them on offboarding).
- Administrative Load: Does the feature reduce the number of helpdesk tickets or the complexity of administration?
- Medium Priority Example: Self-service password reset or an improved user search function for IT admins.