Identity and Access Management System

Aim:

To develop a comprehensive, secure, and scalable Identity and Access Management (IAM) system specifically designed for online banking platforms. The system aims to enhance user authentication and authorization processes, offering robust access control measures while maintaining a seamless user experience in high-security cloud environments.

Objective:

- Implement secure user authentication with multi-factor authentication (MFA) using OTPs and QR codes.
- Design role-based access control (RBAC) to provide Admin, Manager, and Customer dashboards with appropriate access levels.
- Ensure audit logging for all user activities to support monitoring and compliance.
- Develop customizable account lockout mechanisms and emergency login options to enhance security and user convenience.

Scope of the project:

• Tailored User Dashboards:

Separate dashboards for Admin, Manager, and Customer roles to ensure each role has access only to relevant features and information.

• OTP-Based Authentication:

Implementation of two-factor authentication using OTPs (sent via SMS or email) to enhance login security.

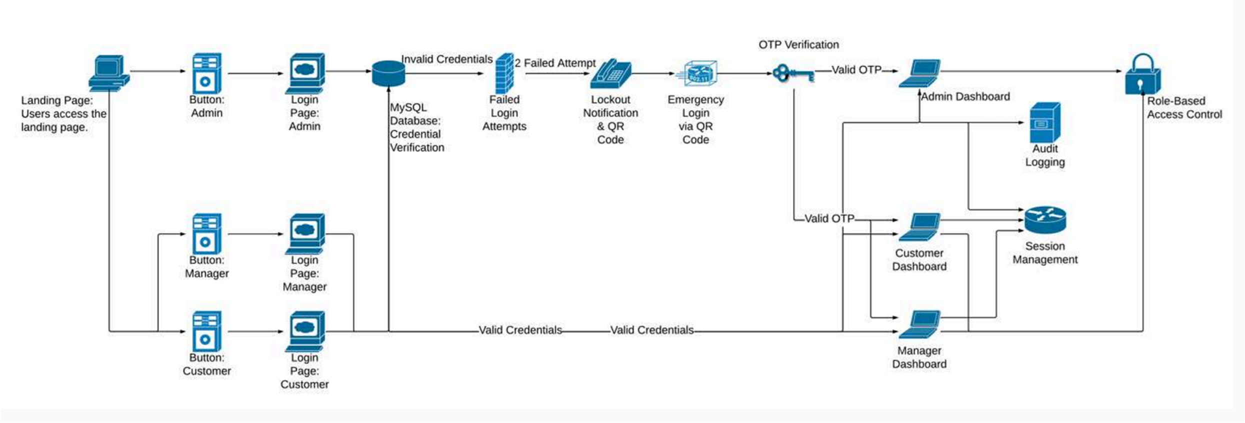
• Comprehensive Audit Logs:

Detailed logging of user actions (e.g., login attempts, role changes, access to sensitive data) for full traceability and compliance with regulatory standards.

- **Enhanced Security Measures:**
Incorporation of advanced security features like customizable account lockout mechanisms, multi-factor authentication, and QR-code-based emergency login for added protection.

- **Role-Based Access Control (RBAC):**
Using RBAC to limit access according to user roles (Admin, Manager, Customer), thus minimizing the risk of unauthorized access.

Proposed methodology:



Tech stack:

Frontend	HTML, CSS, JavaScript
Backend	Django framework in python
Database	Mysql
API Integration	Restful API
Multi-Factor Authentication	Twilio
Emergency Login Mechanism	QR Code Generation

Project Overview:

My Identity & Access Management System is a banking application designed to provide secure authentication and secure transactions. The system has three dashboards: Admin, Manager, and Customer.

- **Admin** can view and add customers, managers, and transactions.
- M**anager** can view and add customers and transactions.
- **Customer** can view their own transactions only.

I implemented key IAM features such as:

- Username & password authentication
- OTP-based multi-factor authentication
- Role-based access control
- Password policies
- Account lockout mechanisms

The **novelty of the project** is the emergency account unlock mechanism.
In traditional banking IAM systems, if an account is locked due to failed attempts, the user needs to visit the bank physically to unlock the account. This is not practical during emergencies.

To solve this, I implemented a **QR-code based emergency unlock system**.
The QR contains a secret device code linked to the user's mobile. During the first setup, the secret code is verified and stored in the database.

If the user gets locked out during an emergency, they can scan the QR code from the web page using their registered device. The system checks three conditions:

1. The secret code must match with the database
2. The device used must be the registered mobile
3. Both the device and web app must be on the same network to prevent fraudulent access

Only if these conditions match, the account is unlocked and login is allowed.
This solution improves usability while maintaining strong security.