IAM Security Solution

Company Details

- Name : TechCorp
- Work : Provide digital solution for other IT company.
- Employees: 150,000+
- Countries: Operating in over 100 countries.

Requirement of Company

- TechCorp seeks to enhance their cybersecurity by improving IAM solutions.
- They want to enhance the user lifecycle management and implement access control mechanism on their system.

Enhancing User Experience and LifeCycle Management :

- Company faced problem from user side when they try to perform onboarding and offboarding task.
- They want to integrate the quick and secure solution for provisioning and de-provisioning.

Improve Access Control Management :

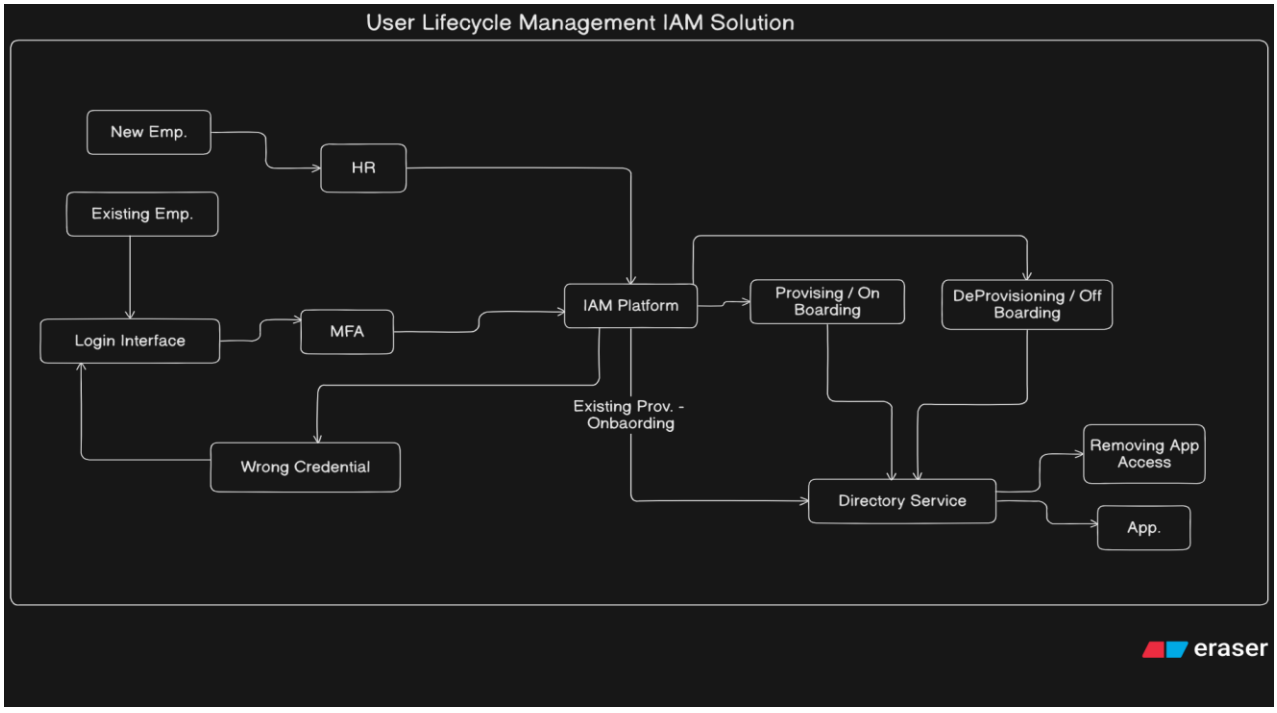
- TechCorp want to integrate MFA (Multifactor Authentication) for add an extra layer of security.
- They required RBAC system for user role based access control. User can access only those data which falls under their category.
- Implement access control mechanism to safeguard critical data and system.

Available Tools and Technology to integrated IAM :

- **Identity Providers (IdP)** → Okta, Microsoft Entra ID (Azure AD)
- **Directory Services** → Active Directory (AD)
- **Single Sign-On (SSO)** → SAML, OAuth 2.0, OpenID Connect
- **MFA Providers** → Google Authenticator, Microsoft Authenticator
- **IAM Automation** → SCIM (System for Cross-domain Identity Management), SailPoint.

Those are some Tools and technology to implement and automate IAM solution.

User LifeCycle Management IAM Workflow :



Technology and Tools are used for that :

- I am not familiar with those tool and technology so I gain knowledge from chatGPT and then I Write it down here :

- But my diagram are cleared with concept becaused I analyze the work and do research on it after I make this diagram

User LifeCycle Workflow Explanation

- My workflow is compatible for TechCorp's requirement.
- HR System can manipulate all employees' data and their credentials.
- HR has direct access to IAM platform to automate the basic and advanced tasks for users or user security.
- The main advantage of this workflow is higher authority can add, alter and delete the particular employee credential if this employee is leaving the company.
- IAM Platform is the main center system for managing security and verifying user credentials.
- IAM Platform automates the provisioning and de-provisioning or onboarding to prevent manual setup or workload.
- Directory Service stores all necessary roles, attributes, and their relationships like RBAC and ABAC.
- Directory Services can provide various tasks and roles according to HR's orders, which can be directly overwritten or changed by HR or higher authority.
- MFA adds a layer of security to prevent unauthorized persons or intruders.
- When an authorized or existing employee tries to access the application, IAM automatically navigates to the application interface without extra steps because the person is already registered and verified.

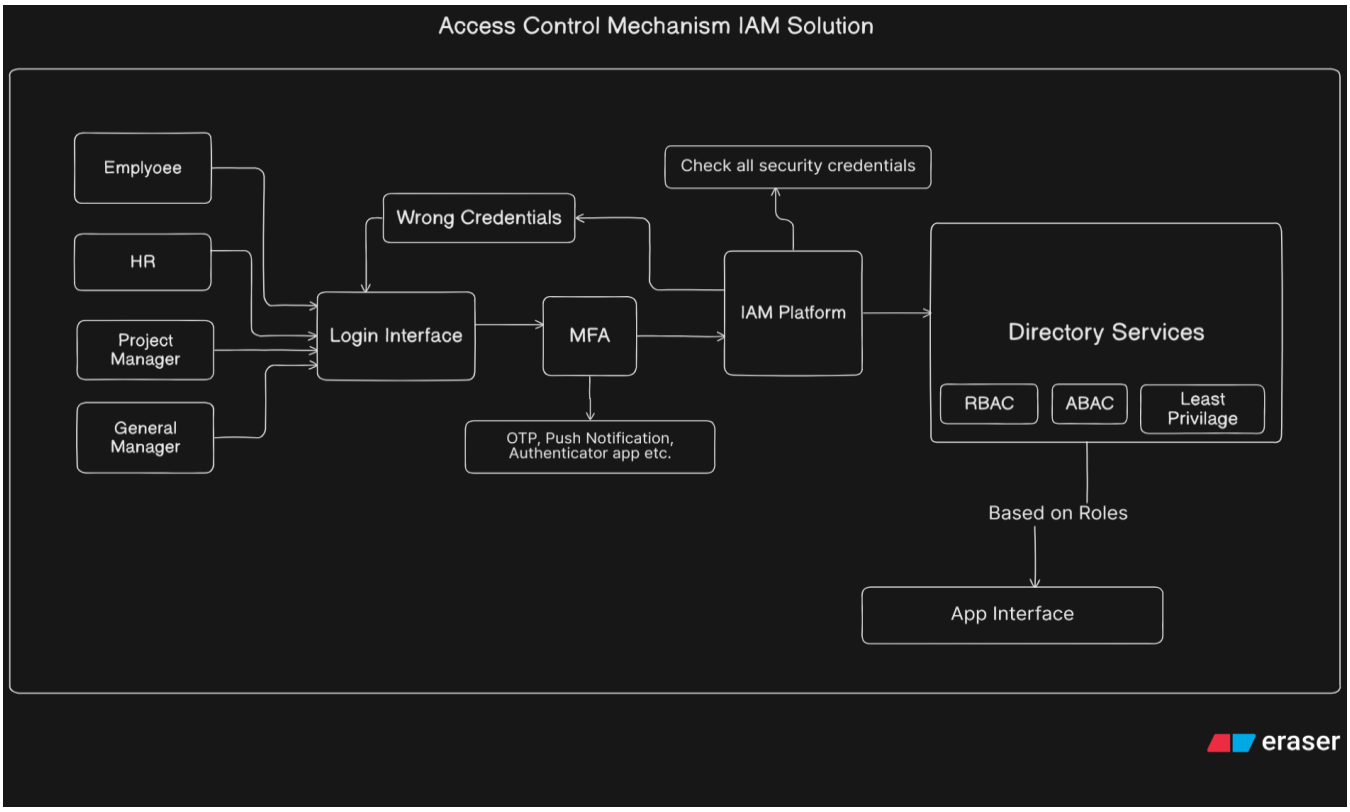
Overcome the Situation

- This Lifecycle can overcome the problem of Techcorp.
- This lifecycle can adds and extra layer of security in user module and prevent unauthorized entity.
- It enhance the User experience if employee is already registered and verified then with minimal security process they can access their resource which allocated by HR.
- If any employee can leave the company then without manual process HR can de-provisioning their role and their credentials with the help of IAM automation tools.

Rationale

This is approach is perfect for prevention of unauthorized activity and streamline user experience with minimal interfering.

Access Control Mechanism



Access Mechanism Workflow Explanation

- This is the Access Mechanism Workflow which is fullfill the TechCorp Requirement.

- Basic Problem is solved by this workflow is Unauthorised person can’t access the legit user data and Each and every user can access only those data or resources which is legal for that.
- Multi Factor Authentication is the extra layer of security which helps to prevent data stolen
- Any kind of user either it is HR or Project Manager or CEO they must passed through the MFA process.
- IAM Platform checks the credential of provided information.
- Directory Manager can checks the role of access required user.
- Directory Manager can verify that only those data access to user that is belong to that person, means An Employee can’t access those data which data accessed and altered by Project Manager.
- Does that mean role based access can prevent unwanted data changes or altered.
- After RBAC verification user navigate to Application interface.

Overcome the Situation

- Unauthorized or Unwanted person can’t access the legal data which is belong to some higher authority person.
- Role Based Access can prevent data altered or deletion.
- All magic handled by Directory management which is important intermediate system of IAM.

Rationale

- This approach can add one more layer of security with directory manager so nobody can access others data or information.