UNIT V ~~PREDICTING HUMAN BEHAVIOR AND PRIVACY ISSUES~~ .

Unit V Understand the access control requirements for social network, Enforcing Access Control strategies, Authentication and Authorization, Roles-based Access Control, Host, Storage and network access control options, Firewalls, Authentication and Authorization Social Network, Identity & Access Management, Single Sign-on, Identity federation, Identity providers and service Consumers, The role of Identity Provisioning.

5.1 Understand the access control requirements for social Network.

→ Access control for social networks typically involves several key components to ensure the security and privacy of user data.

1. User Authentication :-

⇒ Verify the identity of users before granting access to the platform. This can include username/password combinations, two-factor authentication, or biometric authentication.

2. Role-based Access Control (RBAC)

⇒ Assign different roles of users (eg regular user, moderator, administrator) and restrict access to certain features or data based on these roles. This ensure that users only have access to the functionalities

relevant to their role.

3. Privacy Settings :-

⇒ Allow users to control who can view their profile, posts, and other personal information. This may include options to make profiles public, private or accessible to specific groups of users.

4. Data Encryption :-

⇒ Encrypt sensitive data such as passcoords, personal messages, and payment information to prevent unauthorized access, especially during transmission over the network.

5. Session management :-

⇒ Manage user sessions securely, including mechanisms for login / logout, session timeout, and preventing session hijacking.

6. Access Logging and Monitoring :-

⇒ Keep logs of user activity and access attempts for auditing purposes. Monitor access patterns to detect suspicious behavior and potential threats.

7. API Security :-

⇒ Secure API's used for third party integrations to prevent unauthorized access to user data and ensure compliance with privacy regulations.

8. Regular Security Audits:-

⇒ Conduct periodic security assessement and penetration testing to identify and address vulnerabilities in the system.

⇒ By implementing these access control measures, social networks can protect user data, maintain users trust, and comply with relevant privacy regulations such as GDPR or CCPA.

5.2 Enforcing Access control strategies:-

1. Authentication:-

⇒ This is the process of verifying the identity of a ~~system~~ user or system. Common authentication methods include,

* Passwords
* Biometrics (like fingerprints or facial recognition)
* smart cards
* & two factor authentication (2FA), which combines multiple forms of authentication.

2. Authorization:-

⇒ Once a user or system is authenticated, authorization determines what actions they are allowed to perform and what resources they can access.

⇒ This is typically managed through access control list (ACLs) or

Role - based Access control (RBAC) systems, which assign permissions based on roles or individual user Identities.

3. Least Privilege Principle :-

⇒ This principle states that users or systems should only be given the minimum level of access or permissions necessary to perform their tasks. This helps to minimize the potential damage that could result from unauthorized access or misuse of priviledges.

4. Encryption :-

⇒ In addition to controlling access to resources, encryption can be used to protect the confidentiality of sensitive data. This ensures that even if unauthorized access occurs, the data remain unreadable without the proper decryption key.

5. Monitoring and Logging :-

⇒ Implementing and Logging and monitoring mechanisms allow organizations to track access to resources, detect unauthorized or suspicious activities, and respond promptly to security incidents.

⇒ This can include auditing access Logs, setting up alerts for unusual activity, and conducting regular security reviews.

6. Regular Updates and Patching :-

⇒ Keeping software and systems up-to-date with the latest security patches is crucial for maintaining a secure access control environment. Vulnerabilities in software can be exploited by attackers to bypass access controls or gain authorized access to resources.

7. User Education and Training :-

⇒ Educating users about security best practices, such as the importance of strong passwords, avoiding phishing scams, and understanding access control policies, can help prevent security breaches resulting from human error or negligence.

⇒ By implementing these strategies and staying vigilant, organizations can effectively enforce access control measures to protect their sensitive data and resources from unauthorized access or misuse.

5.4. Role- Based Access Control:.

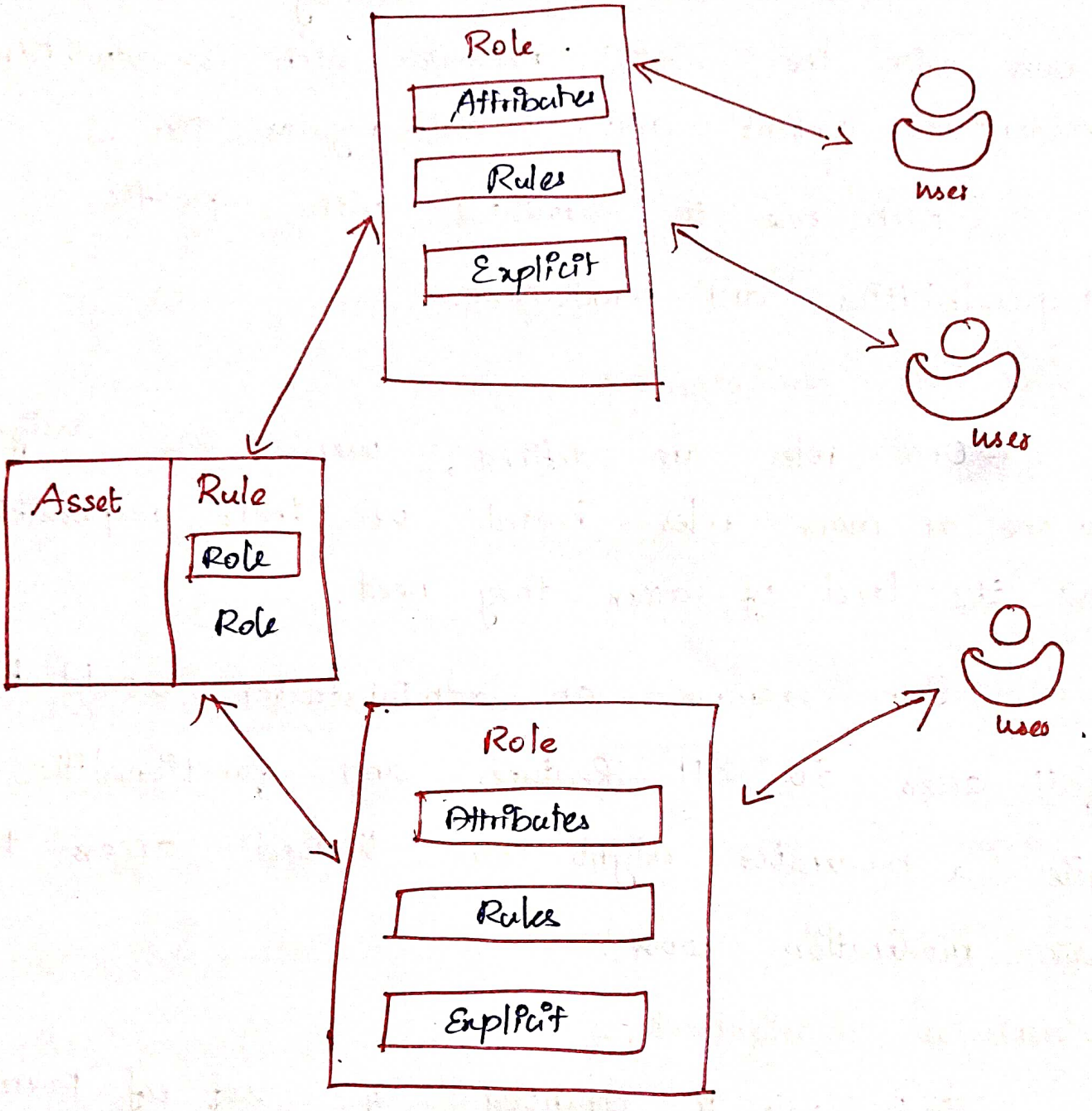
⇒ Roles- based Access control (RBAC) is a crucial component of social network security.

⇒ It helps manage and restrict access to sensitive information by assigning roles to users based on their responsibilities and permissions within the network.

⇒ Admins, moderators, and regular users may have different levels of access, ensuring that only authorized individuals can perform certain actions or access specific data.

⇒ RBAC helps mitigate the risk of unauthorized access, data breaches, and misuse of information within social network.

Working of Role- Based Access Control:



Working of Role-Based Access Control:-

1. Role Assignment:

⇒ RBAC starts with defining different roles with the social network such as administrators, moderators, content creators, and regular users.

⇒ Each role is associated with specific responsibilities and permissions.

2. User Role Assignment:-

⇒ Once roles are defined, users are assigned to one or more roles based on their responsibilities and the level of access they need.

⇒ For example an administrator would have full access to all features and functionalities while a moderator might have limited access to certain moderation tools.

3. Permission Assignment:-

⇒ Each role is granted a set of permissions that define what actions users in that role can perform within the social network.

⇒ Permissions can include creating, editing, or deleting content, moderating user interaction, managing user accounts, and accessing certain features of data.

4. Access Control :-

⇒ RBAC enforces access control by allowing users to perform only the actions permitted by their assigned role.

⇒ This means that users can only access certain features, perform specific actions, or view certain data based on their roles permissions.

5. Dynamic Role Assignment :-

⇒ In some cases, RBAC allows for dynamic role assignment based on user attributes or context.

⇒ For eg, a user's role might change based on the seniority, department, or location with in the organization.

6. Auditing and Monitoring :-

⇒ RBAC systems often include auditing and monitoring capabilities to track users activity and ensure compliance with security policies.

⇒ This helps detect any unauthorized access attempts or suspicious behavior within the

social network.

⇒ Overall, RBAC provides a structured approach to managing access to resources within a social network, reducing the risk of data breaches, unauthorized access, and insider threats while ensuring that users have the appropriate level of access to perform their tasks effectively.

5.3 Authentication and Authorization:-

Authentication :-

⇒ In the authentication process, the identity of users are checked for providing the access to the system.

Authorization :-

⇒ While in Authorization process, the person's or user's authorities are checked for accessing the resources. In the authentication process, users or persons are verified.

Authentication.:-

⇒ Authentication is the process of verifying an identity. It typically requires the use of credentials such as passwords, biometric data, or one-time passcodes. Although the industry is increasingly moving towards passwordless authentication technology.

⇒ Implementing robust authentication mechanisms, such as multi-factor authentication (MFA) and single sign-on (SSO), is essential for protecting user data and streamlining access across multiple platforms.

⇒ MFA is a security measure that requires you to provide more than one piece of evidence to verify your identity, such as a security token or fingerprint.

SSO allows you to authenticate your identity once, and then access other resources available to you, without the need for signing on to multiple systems.

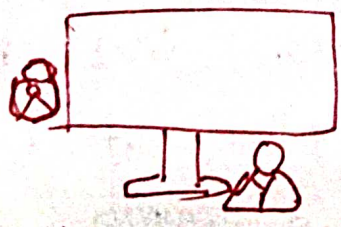
Authorization :-

→ The terms authentication and authorization are often confused. Its understandable. To the end users, they are generally experienced as a single flow or journey. They do, however, serve distinct functions.

⇒ Authentication is the act of verifying identity, ensuring that users or digital entities are indeed who (or what) they claim to be.

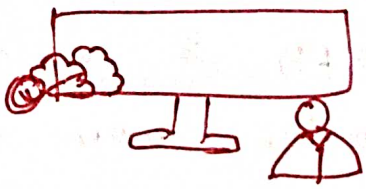
⇒ ~~Authent~~ Authorization, on the other hand, validates and determines the level of access that an authenticated user, machine, or software component has been granted for a specific resource. Essentially, it defines what a verified user or digital identity is permitted to do with in the system

Authentication



confirms users are who they say they are

Authorization



Validates users have permission to complete the attempted action.

5.4. Firewall :

⇒ It is a virtual barrier that helps to protect your devia from authorized acces, but it doesnot directly address privacy issues.

⇒ In the context of social n/w security, a firewall plays a limited role compared to its function in traditional n/w security.

Firewall's Involvement In social Network security.

1. Network Protection :-

⇒ Social Networks host vast amount of user data on their servers. Firewalls are crucial for protecting these servers from external threats such as hackers, malware and DOos attack.

⇒ By filtering incoming and outgoing traffic, Firewalls can prevent unauthorized acces and defend against various cyber threats.

2. Platform Security :-

⇒ Social Network ~~Security~~ platforms themselves deploy firewalls to safeguard their Infrastructure, Including database, servers, and communication channels.

These firewalls help to prevent unauthorized accen to sensitive user information stored within the

platforms' systems.

Techniques or Approaches.

1. Privacy settings:

⇒ Social Network users should carefully configure their privacy settings to control who can see their posts, photos and personal information. These settings dictate the visibility of content and limit access to personal data.

2. Data Encryption:

⇒ Social Network should employ strong encryption methods to secure user data in transit and at rest. This prevents authorized parties from accessing sensitive information exchanged between users and platforms' servers.

3. User Education:

⇒ Users should be educated about the risks associated with sharing personal information on social networks and encouraged to exercise caution when interacting with unknown parties or third party applications.

⇒ Protecting privacy on social Network ~~involves~~ includes these Approaches by firewalls.

5.7 Identity and Access Management (IAM)

⇒ IAM is crucial for protecting data and ensuring that only authorized users, machines, and applications get access to the right resources, at the right time. It's an essential part of ensuring secure and efficient system interactions.

Basic concepts:-

⇒ Resource:- It is a digital asset that requires protection and controlled access. Eg Include, files, databases, Web applications, APIs, devices, or services.

⇒ User:- It is someone represented by a digital identity, who wants to access a resource or group of resources.

⇒ For eg:- Customer, partner, member., or employ

A digita identity can also represent a non-human. such as machine, applicatpon or workload.

Core functions of Identity and Access Management :-

⇒ Identity and Access Management is a framework of policies and technologies that gives verified users or digital or digital entities ~~that~~ the appropriate level of secure access to resources, such as email, databases and applications.

⇒ It involves the identification, authentication and authorization of entities to have access to resources by associating permissions and restrictions with digital identities.

Core functionality :-

1. Identity Management :-

⇒ creating, storing, and managing users' digital identities, including monitoring their permissions and access levels.

2. Identity Federation :-

⇒ Enabling access across systems, allowing users to use existing credentials for new services, such as getting access to your systems.

3 Provisioning and Deprovisioning :-

⇒ Managing the User account life cycle, assigning or revoking access to resources and permission levels.

4 Authentication and Authorization :-

⇒ Validating identities and granting appropriate Access rights.

5 Access Control :-

⇒ Defining and enforcing who or what has access to which resources. Regulating access to systems and data.

6. Reporting and Monitoring :-

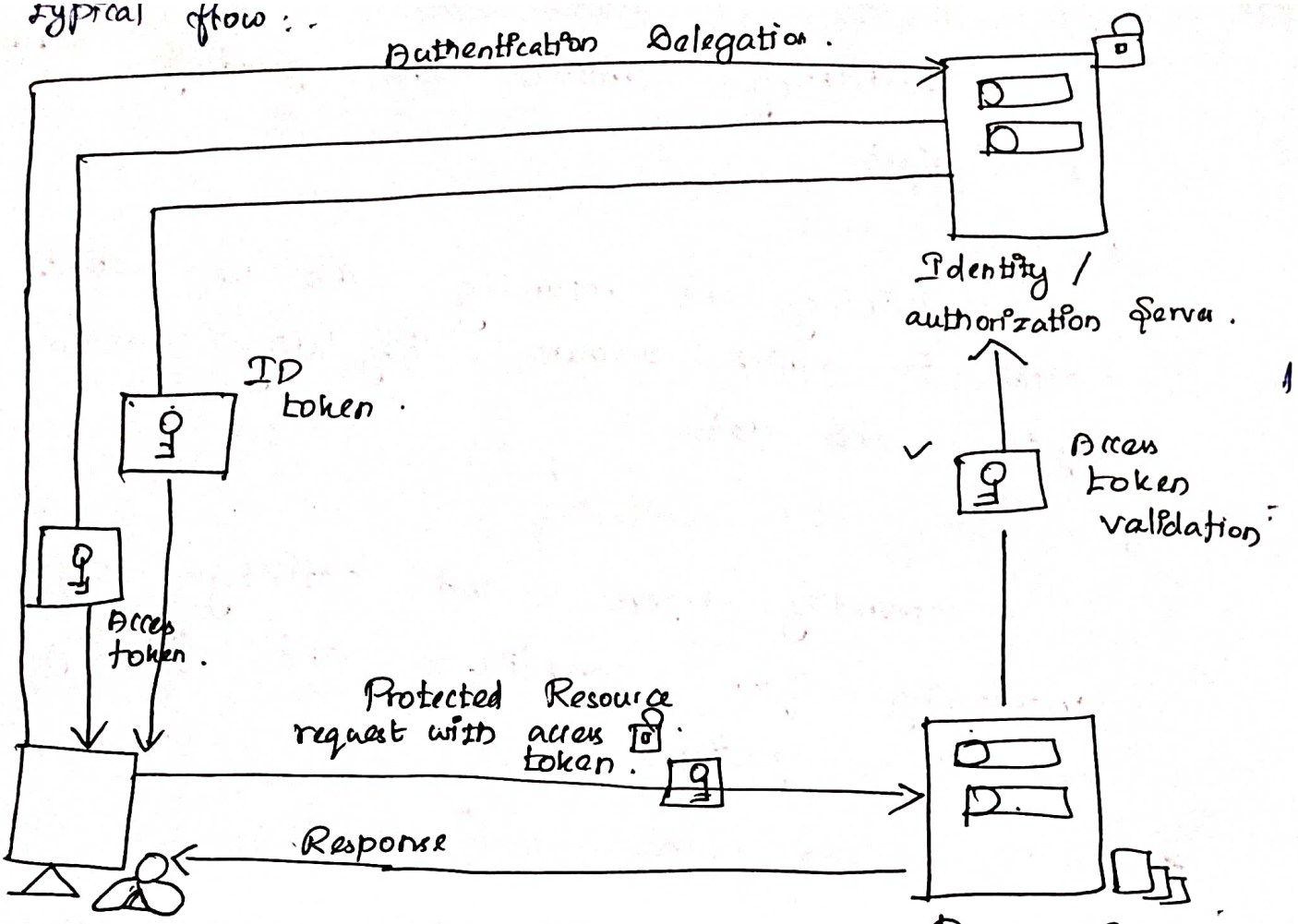
⇒ Generating reports and activity logs and monitoring for compliance and security purposes and usage patterns.

* Identity Access Management Working :-

⇒ Identity Access Management — Creation, storing, and management of identity information and the regulating of access through the processes of authentication and authorization.

⇒ IAM encompasses a broad range of systems and approaches - a framework, that orchestrates a series of processes to ensure the secure and efficient management of digital identities and access to resources.

Typical flow :-



Request authentication :-

⇒ The User initiates an authentication request with the identity provider from the client application.

verify credentials :-

⇒ If the user's credentials are successfully verified, the identity provider sends an ID token containing information to the client application.

Grant authorization :-

⇒ The user consents, and the identity provider sends an access token to the client

application :-

Grant authorization :-

⇒ The User consents, and the identity provider sends an access token to the client application, providing access to resources.

Access Resources :-

⇒ The access token is attached to subsequent request to the resource server from client application.

Validate and Respond :-

⇒ The identity provider validates the access token and if valid, grants access to the requested resources and sends back a response to the client application.

5.9 Identity Federation :-

⇒ Identity federation is the process of delegating an individual's or entity's authentication responsibility to a trusted external party.

⇒ Each partner in federation plays the role of either an Identity Provider (IdP) or Service Provider (SP).

⇒ In Identity federation, an IdP vouches for the identity of the users, and an SP provides service to the users.

⇒ When a user wants to access a service of an SP, the SP delegates the authentication to the IdP. This is called federation.

⇒ SP must trust the authentication ability of the IdP. The trusted Identity providers can be on-premise federation services, corporate directories, social Identity providers like Google, Facebook, Twitter etc.

Identity federation working process.

Suppose a user wants to access a secured SaaS application (Software as a Service)

that requires the user to be authenticated.

1) The user navigates to the application of SP.

2) SP requires the user to be authenticated at the IdP (SP may have mechanisms to check whether the user is currently authenticated at the IdP using session data).

The unauthenticated user is redirected to login page of the IdP.

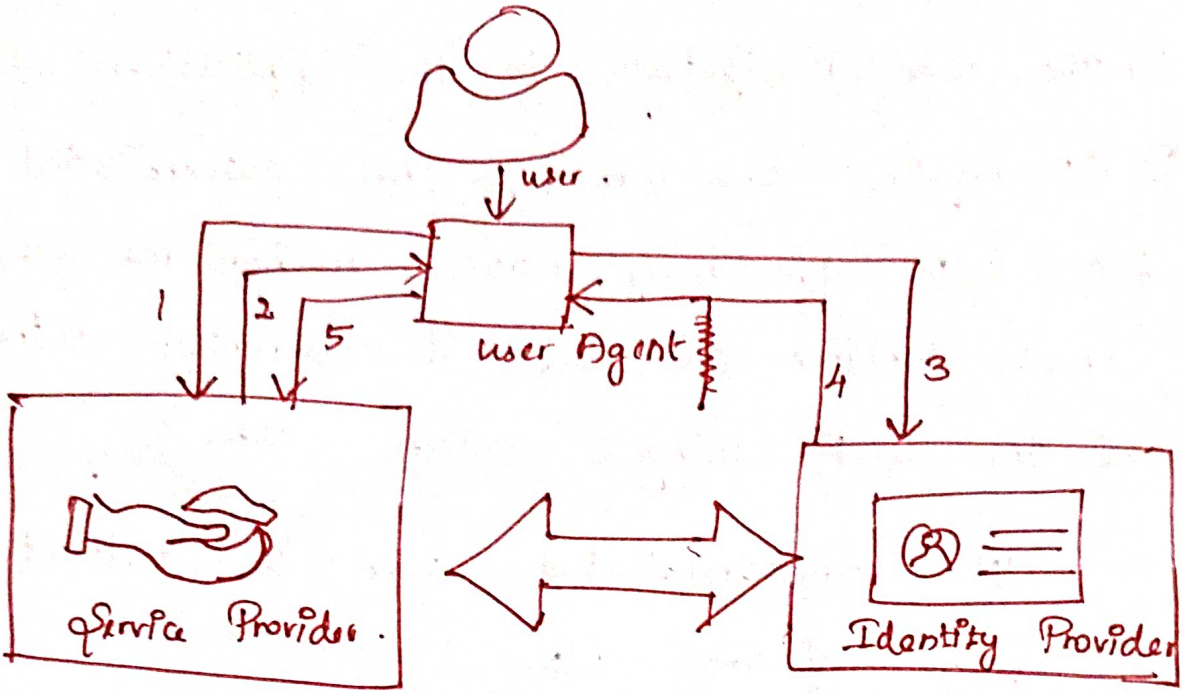
3). The user authenticates with the IdP (by entering login credentials)

4) If the user credentials are properly validated the user is authenticated and provided an access token.

5) The user goes back to the application with the obtained access token and the application allows the user to access the application.

Benefits of Identity Federation:

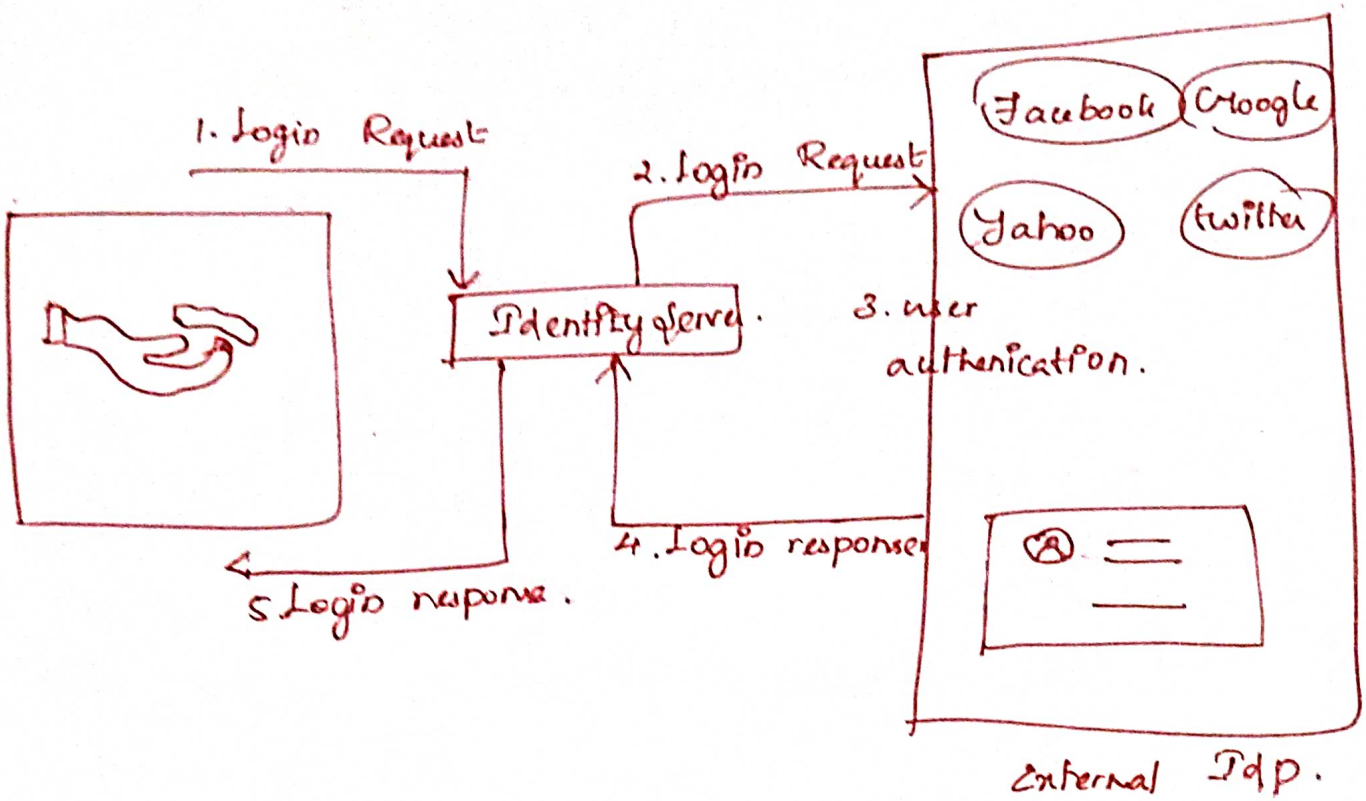
⇒ Identity federation saves end users from the burden of remembering multiple ~~user~~ sets of credentials for each and every service application (either cloud or on-premise ~~for~~ application) they consume.



Identity Federation : . Process Flow .

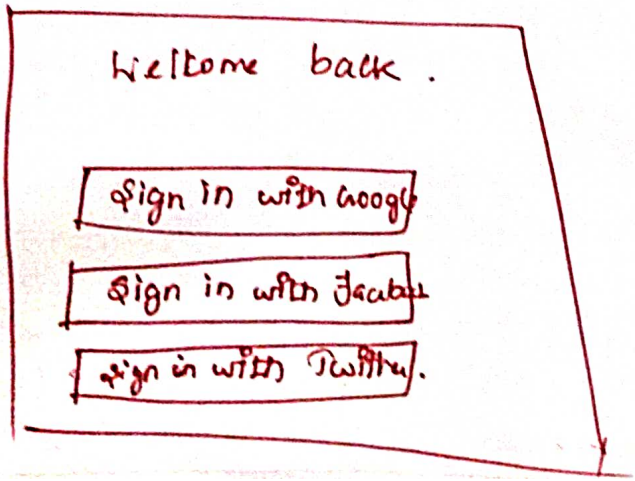
IAM supports two types of Identity federation.

1. Enterprise Identity federation.
   - ⇒ SAML (Microsoft Active Directory)
   - ⇒ Custom & Federation Broker.
2. Web Identity Federation.
   - ⇒ Amazon
   - ⇒ Facebook.
   - ⇒ Google
   - ⇒ open ID connect (OIDC) 2.0.



⇒ IdP allows you to authenticate with a third party service like Google, Facebook or Twitter as the Identity provider.

⇒ When you sign in to Medium by clicking "sign in with Google" (or with Facebook / Twitter) Google (or Facebook / Twitter) acts as the trusted IdP that authenticates you on behalf of Medium and relays the authentication decision to Medium.



5.8 Single Sign-on (SSO)

⇒ It is an authentication tool that enables users to securely access multiple applications and services using one set of credentials, eliminating the need to remember different passcoords for each service.

What is SSO?

Single sign-on (SSO) is like having a master key for all your apps - it lets you log in once and access multiple applications without needing to enter your password again.

How does it work:-

⇒ When you log in to one application using SSO, it store your credentials securely, Then when you try to access another app, SSO automatically logs you in without asking for your username and password again.

Benefits of SSO:-

1. SSO and Social Network:-

Social networks like facebook, or Google let you use your account to log in to other websites or apps without making new acounts or ~~rembem~~ remembering extra passwords.

2. Convenience :-

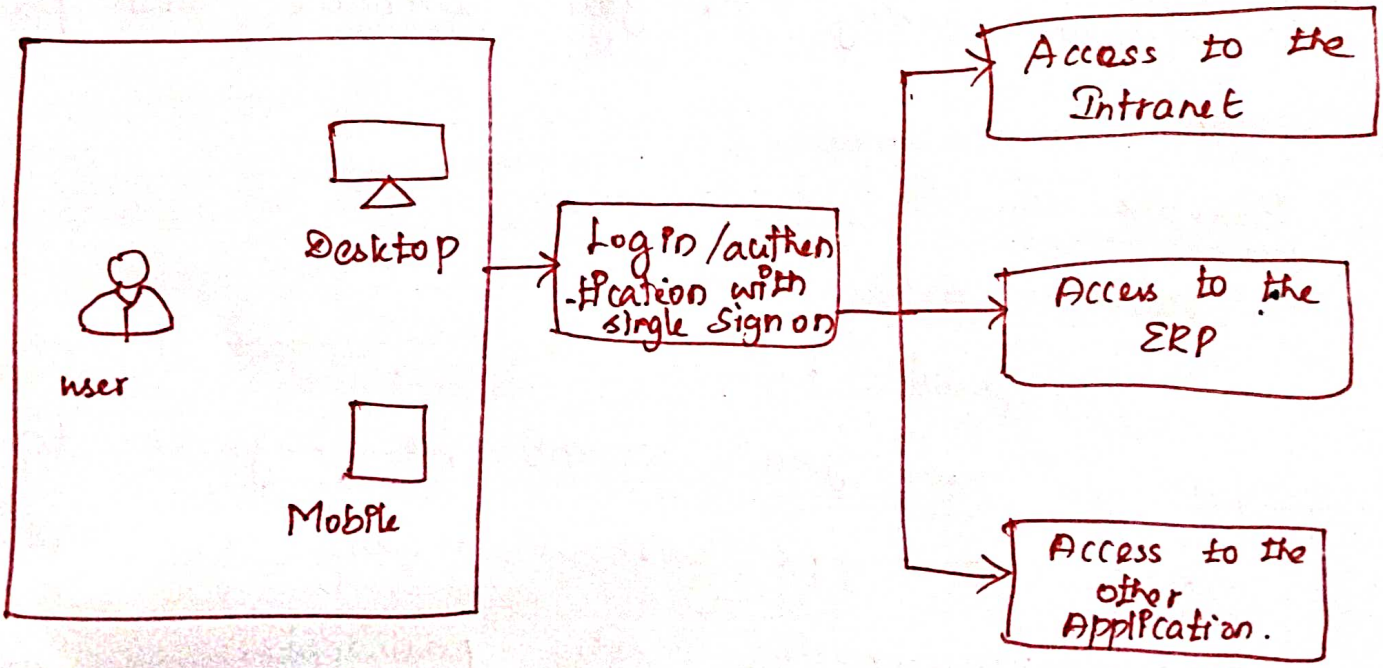
It's easier because you only need to use your social media login instead of creating new accounts everywhere you go.

3. Better Experience :-

This makes things smoother because you don't have to keep track of lots of usernames and passwords for different sites.

4. Privacy Check :-

But remember, when you use social media logins, some of your information might be shared with the website or app, so it's good to be aware of what's being shared.



Architecture of Single Sign-on.

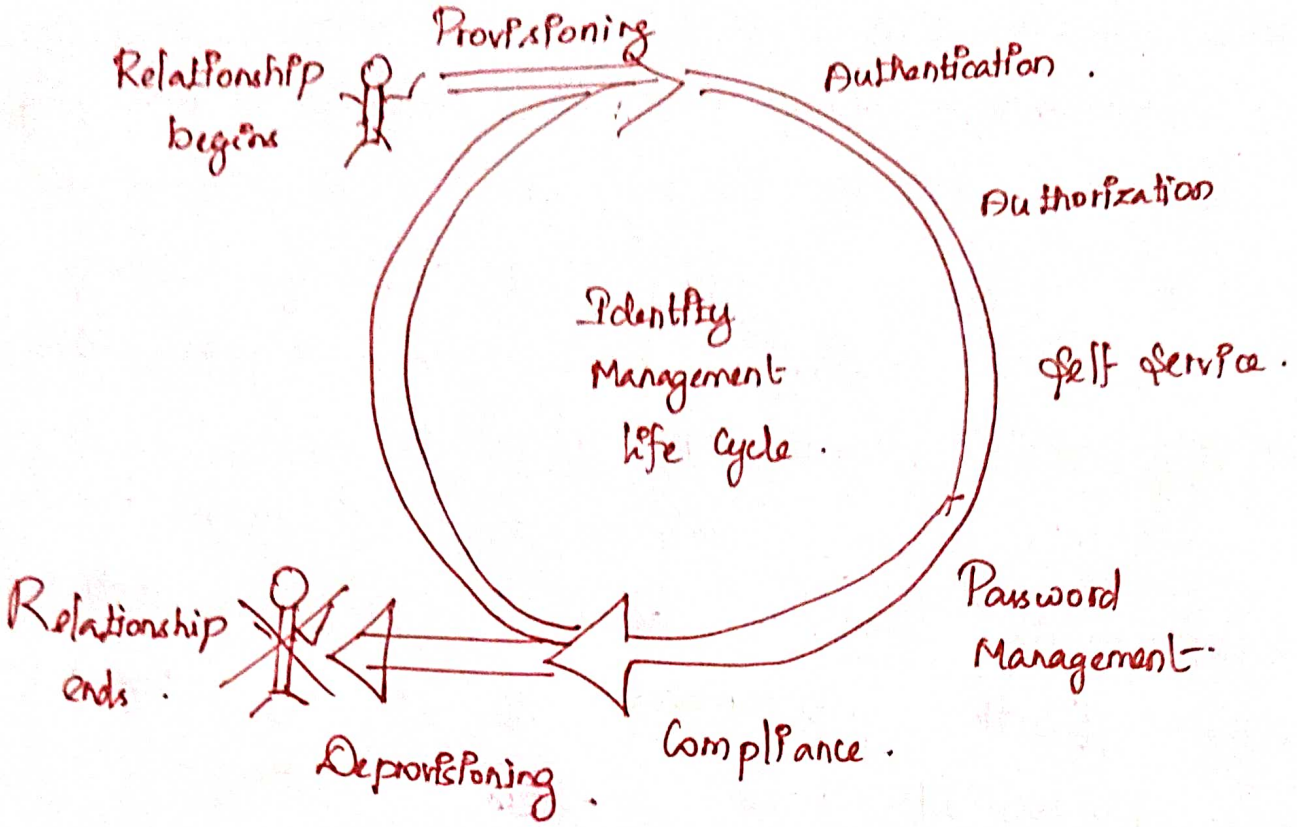
5.b. Role of Identity Provisioning :-

⇒ Identity provisioning is crucial in managing access to resources within an organization. It involves creating, managing and revoking user identities and their associated access rights to various systems and applications.

⇒ This process ensures that individuals have the appropriate level of access to perform their job duties efficiently while maintaining security by preventing unauthorized access.

⇒ Identity provisioning typically includes tasks such as user account creation, modification, and deprovisioning as well as assigning roles and permissions based on job responsibilities.

⇒ It plays a significant role in maintaining security, compliance and operational efficiency within an organization.


Provisioning
Relationship begins
Authentication
Authorization
Identity Management life cycle.
Self service.
Password Management.
Compliance.
Deprovisioning.
Relationship ends.