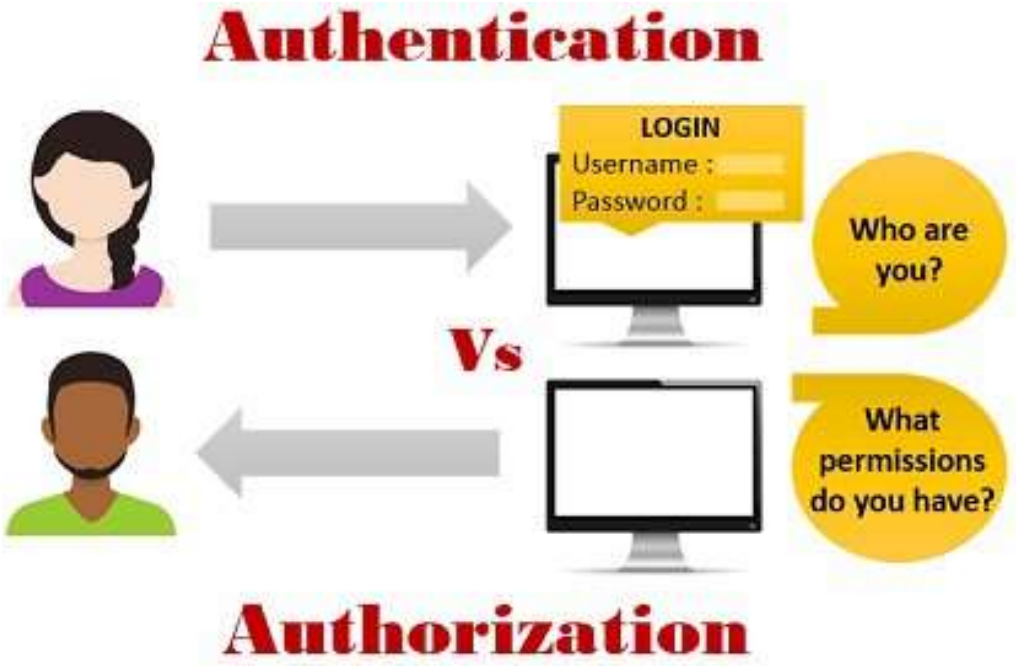
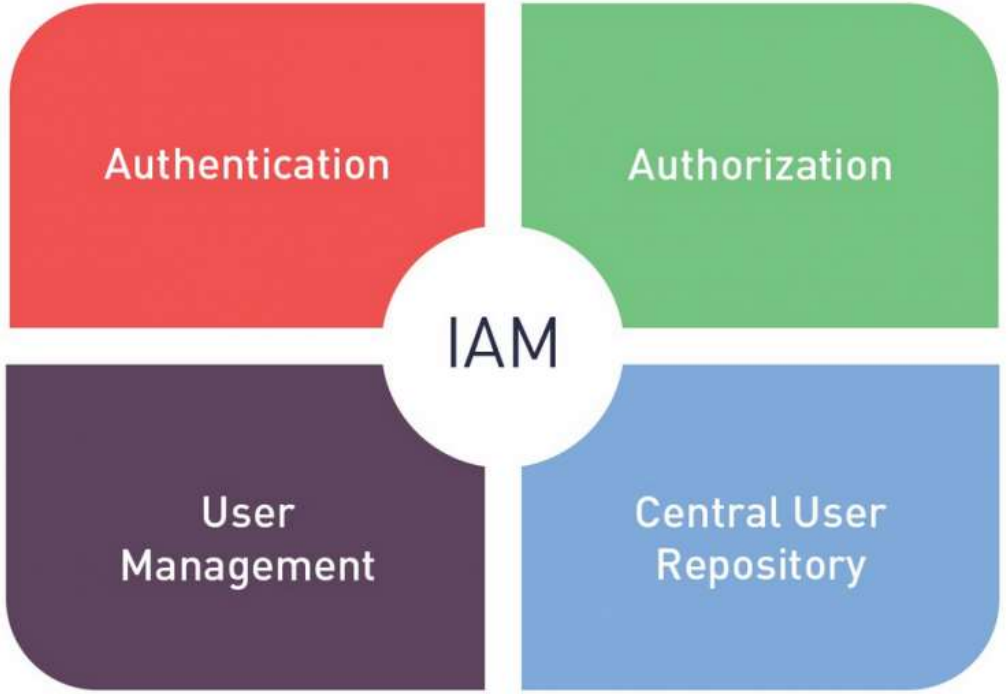
# DEPARTMENT OF COMPUTER APPLICATIONS

| COURSE | UNIT V | TOPIC | Semester |
|---|---|---|---|
| 23CAE717 Cloud Computing | **Security in the Cloud** | **Identity and Access Management** | II Semester / I MCA |

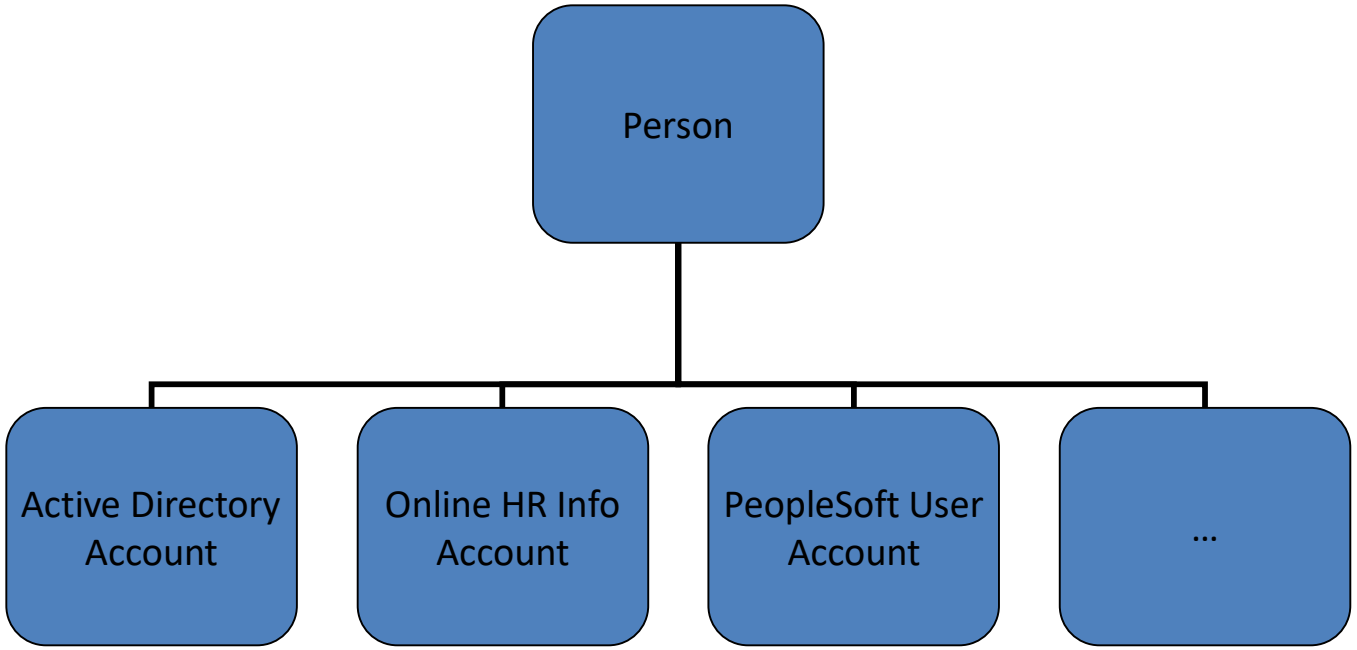
# Authentication and Authorization




## Identity and Access Management

# Identity and Access Management





- Networks use multiple identity systems
- Users get confused with all of these Ids
- Management and audit has difficulty keeping track of all these Ids

# Identity Management

- Management of individual identities, their authentication, authorization, roles and privileges/permission within or across system boundaries with goal increasing security and productivity

- Solution should cover
  - Single identify
  - Multiple identity
  - Service/batch identity
  - Cloud identity

# Identity and Access Management

- Enable right individual to access right resources at right time for right reasons
- Secure way to distribute resources across network

# Why IAM ?

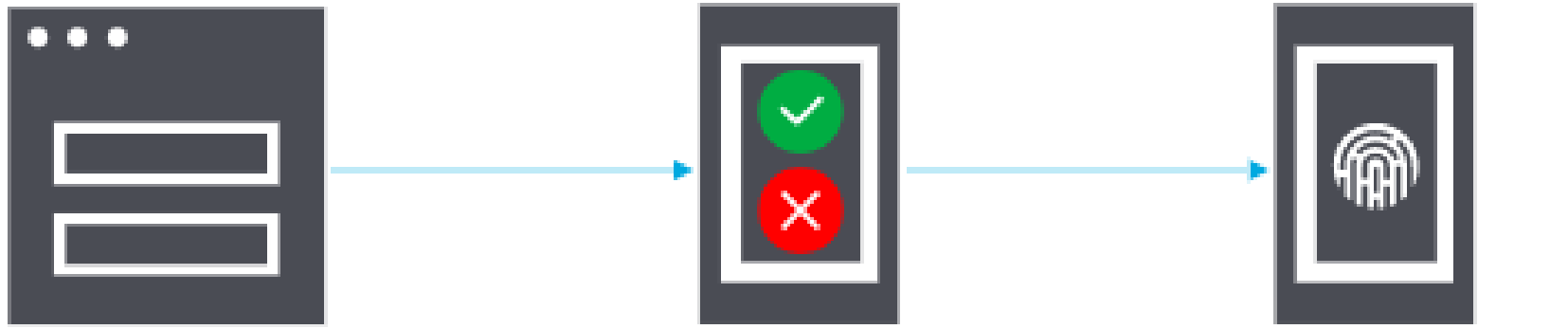
- Weak passwords – eliminate using single sign-on
- Single identity
- Centralized access control –access through secure channel
- Multi factor authentication - additional layer of security
- Phishing
- Integrated Application management
- Password reset – eliminated
- Facilitate data analytics

# Identity and Access Management

- Multi-factor Authentication (MFA)

  Most MFA authentication methodology is based on one of three types of additional information:

  1. Things you know (knowledge), such as a password or PIN
  2. Things you have (possession), such as a badge or smartphone
  3. Things you are (inherence), such as a biometric like fingerprints or voice recognition



**Step 1:** User name and password entered

**Step 2:** Pin from phone app entered

**Step 3:** Fingerprint verified

# MFA Examples

- KNOWLEDGE
  1. Answers to personal security questions
  2. Password
  3. OTPs (Can be both Knowledge and Possession - You know the OTP and you have to have something in your Possession to get it like your phone)
- POSSESSION
  1. OTPs generated by smartphone apps
  2. OTPs sent via text or email
  3. Access badges, USB devices, Smart Cards or fobs or security keys
  4. Software tokens and certificates
- INHERENCE
  1. Fingerprints, facial recognition, voice, retina or iris scanning or other Biometrics
  2. Behavioral analysis

# Authentication, Authorization, and Accountability (AAA)

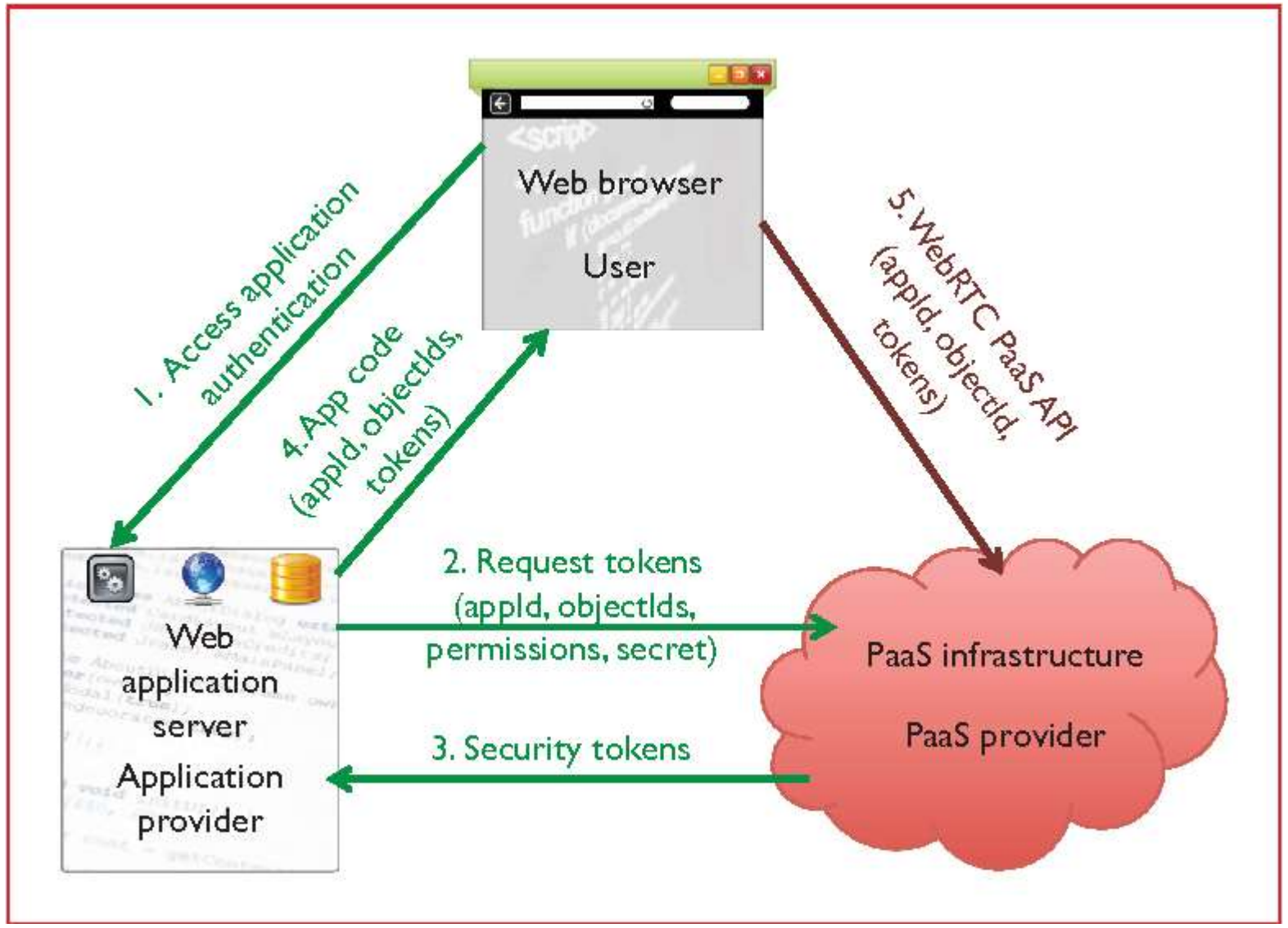
**AAA** is a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for **services**.

**A**uthentication – Who is allowed to access ?

**A**uthorization – What resources are allowed to access ?

**A**ccounting – What is being accessed ?

# Authentication, Authorization, and Accountability (AAA)



# Identity and Access Management

**Initiate, capture, record and management identities**

- Authentication (AuthN)
  - Verify that a person is who they claim to be
  - This is where multi-factor authentication comes into play
  - Identification and authentication are related but not the same
- Authorization (AuthZ)
  - Deciding what resources can be accessed/used by a user
- Accounting
  - Charges you for what you do

**Balance between usability and security**

# IAM standards

- avoid duplication of identity, attributes, and credentials and provide a single sign-on user experience
  - SAML(Security Assertion Markup Lang)
- automatically provision user accounts with cloud services and automate the process of provisioning and deprovisioning
  - SPML (service provisioning markup lang)
- provision user accounts with appropriate privileges and manage entitlements
  - XACML (extensible access control markup lang)
- authorize cloud service X to access my data in cloud service Y without disclosing credentials
  - Oauth (open authentication)

# SAML standards