Exercise: Classifying Requirements

Requirement	Functional Requirement (FR) / Non-Functional Requirement(NFR)
A. The system should display the result of the student within 1 second.	Select one of : [FR/ NFR]
B. The date of birth of the student should be displayed in DD/MM/YYYY format	Select one of : [FR/ NFR]
C. The student portal should support 10,000 students of the university at a given point of time.	Select one of : [FR/ NFR]
D. The university website should be available 99.999 % of the time.	Select one of : [FR/ NFR]
E. The student must be able to download the syllabus of the semester as PDF (Portable Document Format) Files.	Select one of : [FR/ NFR]
F. The system should be menu-driven.	Select one of : [FR/ NFR]
G. 80% of the new students registration must be able to take the details in the database within the first 5 minutes of time.	Select one of : [FR/ NFR]

Case Study 1-GGSIPU's Centralized Authentication System (CAS)

- **Problem Statement**
- As an organization GGSIPU is expanding which leads to the increase in the number of systems, applications, and services that require authentication and authorization. This often leads to a proliferation of disparate authentication systems that may not integrate well with each other. This creates several issues, such as difficulties in managing user credentials, increased risk of security breaches, and inconsistent user experiences.
- Furthermore, maintaining multiple authentication systems can be costly in terms of time, money, and resources. Additionally, different authentication systems may have different security policies, which can make it challenging to ensure compliance with regulations and standards.
- Therefore, there is a need for a GGSIPU's Centralized Authentication System (CAS) that can provide a unified and secure method for authenticating users across all systems, applications, and services within an organization. This system should be able to integrate with existing authentication systems and provide a consistent user experience while also ensuring compliance with security policies and regulations. The purpose of this SRS is to define the requirements for such a CAS.

Introduction

- The purpose of this document is to define the requirements for a CAS that provides a unified and secure method for authenticating users across all systems, applications, and services within an organization. This system will integrate with existing authentication systems and provide a consistent user experience while ensuring compliance with security policies and regulations.

- **Scope**
- The CAS will be a centralized system that will provide authentication and authorization services for all systems, applications, and services within GGSIPU. It will integrate with all future applications and provide a single sign-on (SSO) experience for users.

System Requirements

- **Following are the CAS requirements in detail:**

1. A web-based interface for anytime anywhere access by employees, deans and incharges of respective departments and personnel departments for log in to the CAS and its integrated applications.
2. A single sign on based authentication and authorization system to ensure secure access to the system. It shall be able to provide a dashboard allowing a user to switch between all the integrated applications without providing their credentials.
3. A database to store employees' official information with their official information which is common and which shall be shared across the applications .
4. The ability to provide authentication and authorization services to all the existing and future applications across the GGSIPU digital ecosystem.

- **User Roles**

- The CAS will have the following user roles:

1. Employee: An employee will be able to view their personal and official details and be able to visit the integrated applications through a dashboard as per his authorization.
2. Administrator: An administrator will have full access to the CAS and will be able to configure system settings, manage masters and generate audit reports. The Administrator will also be responsible for the registration, activation of applications and other tasks related to employee management. The Administrator shall also be able to create new roles with overlapping capabilities as per the future requirements.
3. Monitor: This role will have complete viewable access to the entire system without actions. The monitoring user will be able to view the information in rollup and drill down fashion of the entire institute.

Workflow

- The CAS workflow will consist of the following steps:

1. An employee logs into the system and upon login he will be shown a list of integrated applications in the form of a dashboard.
2. On clicking the selected application, he will be redirected to that application's landing page.

- **Security**

The CAS will include the following security measures:

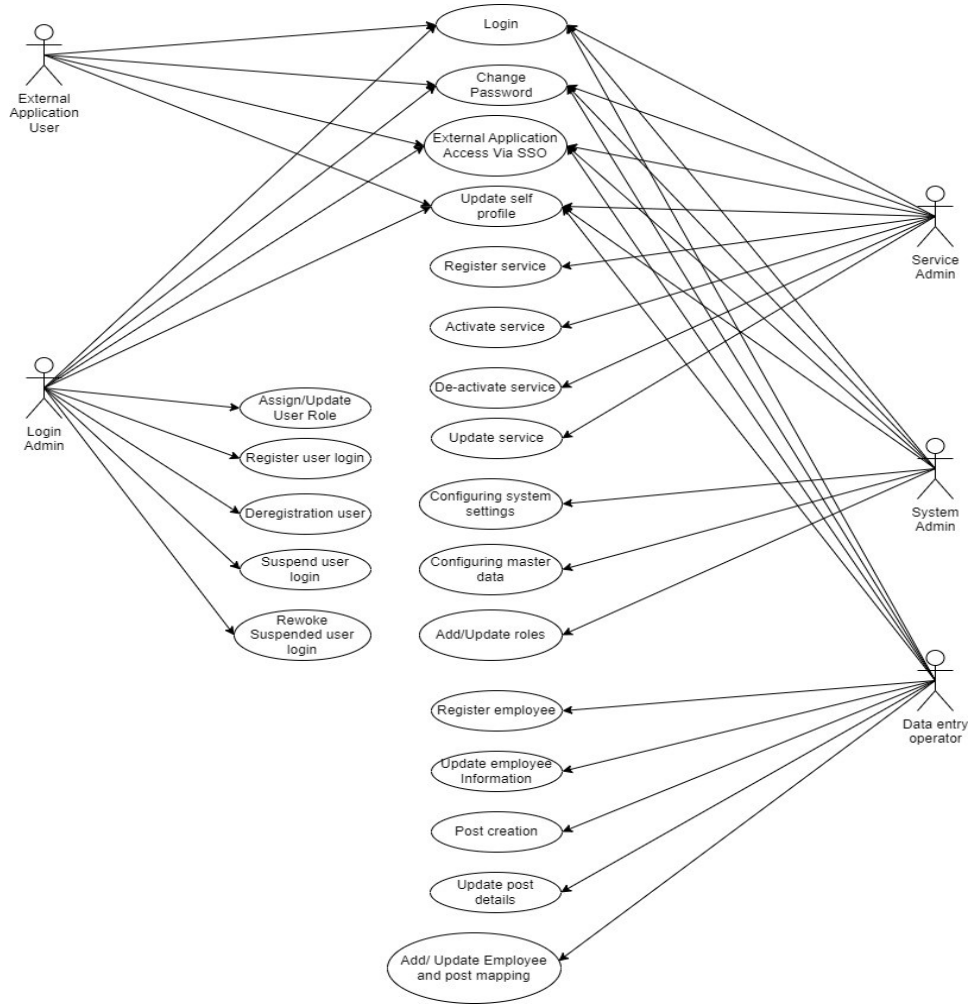
1. Secure login and password management to ensure only authorized users can access the system.
2. Security hardening and session management as per the latest secure coding and session management practices.
3. Hardening of the web server as per the latest available security guidelines.
4. Regular backups of the database to ensure data is not lost in case of a system failure.

Use Case Diagram

- The actors in the CAS are the various individuals or entities that interact with the system to accomplish different tasks. Here are some of the key actors in the CAS:

1. External Application User: This type of user is the primary actor in the CAS. They will log in to the system by providing user credentials such as Username and Password. Once successful login to the system, the user will be provided a list of applications mapped to his user id in the form of a dashboard, and it allows the user to redirect to the application using single sign on facility, i.e. without entering username and password.
2. Login Administrator: The login administrator is responsible for registration and deregister a user login, assigning or modifying a role of a user. He/She will be also responsible for handling the request of unblocking of the user account, if any.
3. Service Administrator: The service administrator is responsible for registration, activation, deactivation of integrated applications with the CAS, including setting up mode of integration, type of security and monitoring of the application logs.
4. System Administrator: The system administrator is responsible for managing the CAS, including setting up the system, managing user access, and generating security compliance reports.
5. Data Entry Operator: The DEO is responsible for entering/updating employee details, post creation/updation, allocation and relieving of employees to/from a post, generating employee and post based reports.

Use Case Diagram of CAS



Functional Requirements

1. **User Authentication:** The CAS shall authenticate users based on their username and password credentials. The CAS shall support multi-factor authentication methods, including but not limited to SMS-based one-time passwords (OTP). The CAS shall enforce password policies, including complexity, length, and expiration. The CAS shall support password recovery mechanisms.
2. **User Authorization:** The CAS shall authorize users based on their assigned roles and permissions. The CAS shall support the assignment and management of roles and permissions for users. The CAS shall enforce access control policies for users based on their roles and permissions.
3. **Single Sign-On (SSO):** The CAS shall provide a single sign-on (SSO) experience for users across all future systems, applications, and services. The CAS may support SSO integration with existing authentication systems depending on the technical capability of the existing applications. The CAS shall support session management for SSO and also provide a provision to integrate the applications which requires only one time authentication without SSO features.
4. **Security:** The CAS shall enforce security policies, including but not limited to authentication and authorization policies. The CAS shall use industry-standard encryption algorithms for secure communication. The CAS shall support auditing and logging of authentication and authorization events. The CAS shall comply with applicable security regulations and standards.
5. **Usability:** The CAS shall provide a user-friendly and intuitive interface for authentication and authorization. The CAS shall provide clear and concise error messages for authentication and authorization failures.

Non Functional Requirements

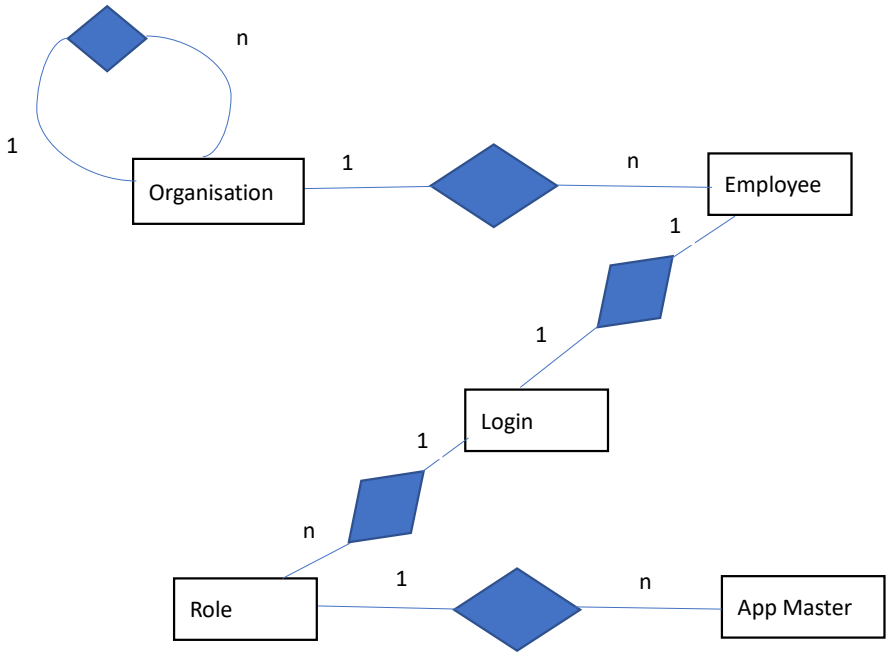
- Non-functional requirements for the CAS for 5000 employees include:

1. **Scalability:** The CAS shall support at least 5000 concurrent users. The CAS shall provide fast and responsive authentication and authorization services. It shall also have the ability to scale up to accommodate additional users as the number of employees grows. The CAS shall support horizontal and vertical scaling.
2. **Performance:** The system should have a response time of no more than 3 seconds for the 99.9% of the time when an employee submits or views their leave application, even during peak usage periods. The CAS shall provide high availability and fault tolerance.
3. **Compatibility** The CAS shall be compatible with existing authentication systems and applications.
4. **Security:** The system should use secure protocols such as HTTPS and have role-based access control to ensure that only authorized personnel have access to employee leave records. The system should comply with the latest CERT security guidelines and pass through all the security audit processes.
5. **Reliability:** The system should have an uptime of at least 99.9% and be able to recover from any failures or disruptions within 30 minutes.
6. **Maintainability:** The system should be designed to be easily maintainable, with documentation provided to guide administrators in performing updates, backups, and maintenance tasks. The system is expected to run 24 X 7, although there would be a scheduled downtime of one hour every month for the regular maintenance activities.
7. **User Experience:** The system should be easy to use, with a simple and intuitive interface that requires no more than 30 minutes of training for new users.
8. **Compliance:** The system should comply with relevant government laws and GGSIPU policies, including rules for managing employee leave entitlements and handling leave requests and approvals.
9. **Integration:** The system should be able to integrate with all the existing division's systems such as payroll and employee data management systems to provide them authentication and authorization services.
10. **Constraints:** The CAS shall be developed using industry-standard software development methodologies and tools. The CAS shall be compatible with the organization's existing technology stack and infrastructure.
11. **Assumptions and Dependencies:** The development and deployment of the CAS will depend on the availability of appropriate hardware and software resources. The CAS will assume that users have appropriate access to systems, applications, and services based on their roles and permissions.

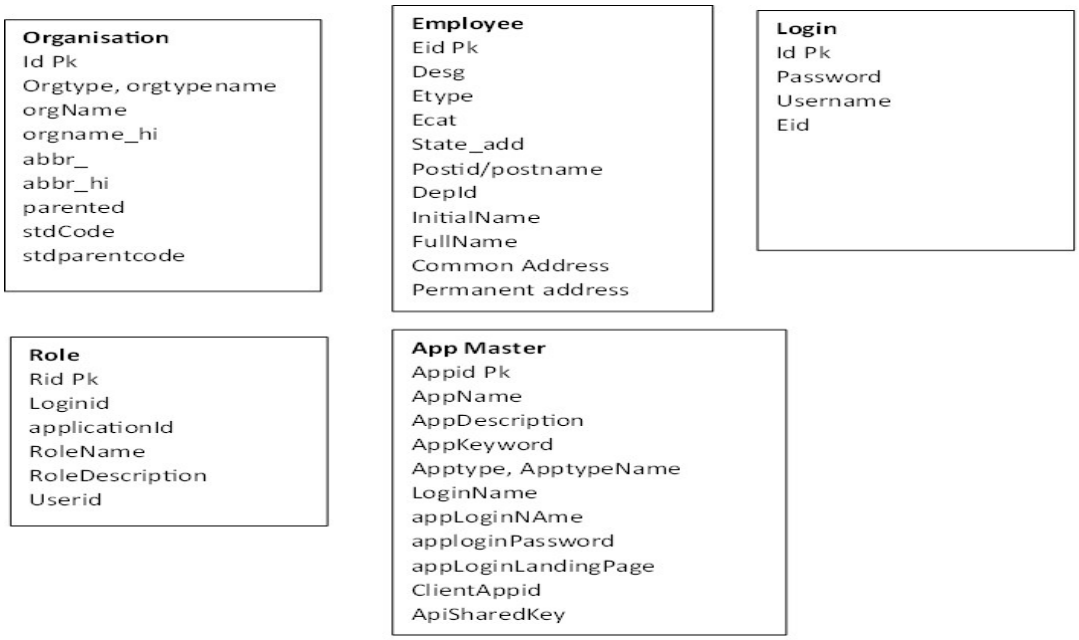
Conclusion

- The Central Authentication System (CAS) will provide a centralized and secure method for authenticating users across all systems, applications, and services within an organization. It will integrate with existing authentication systems and provide a consistent user experience while ensuring compliance with security policies and regulations.

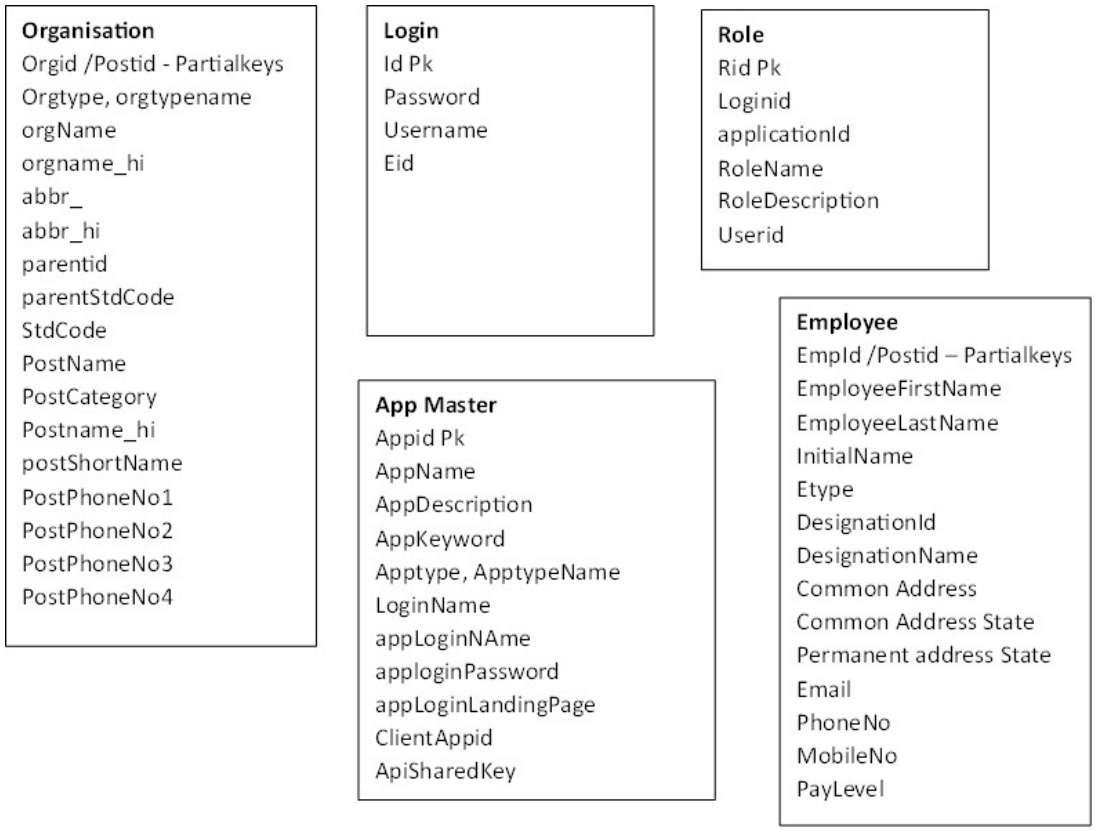
ER Diagram of CAS



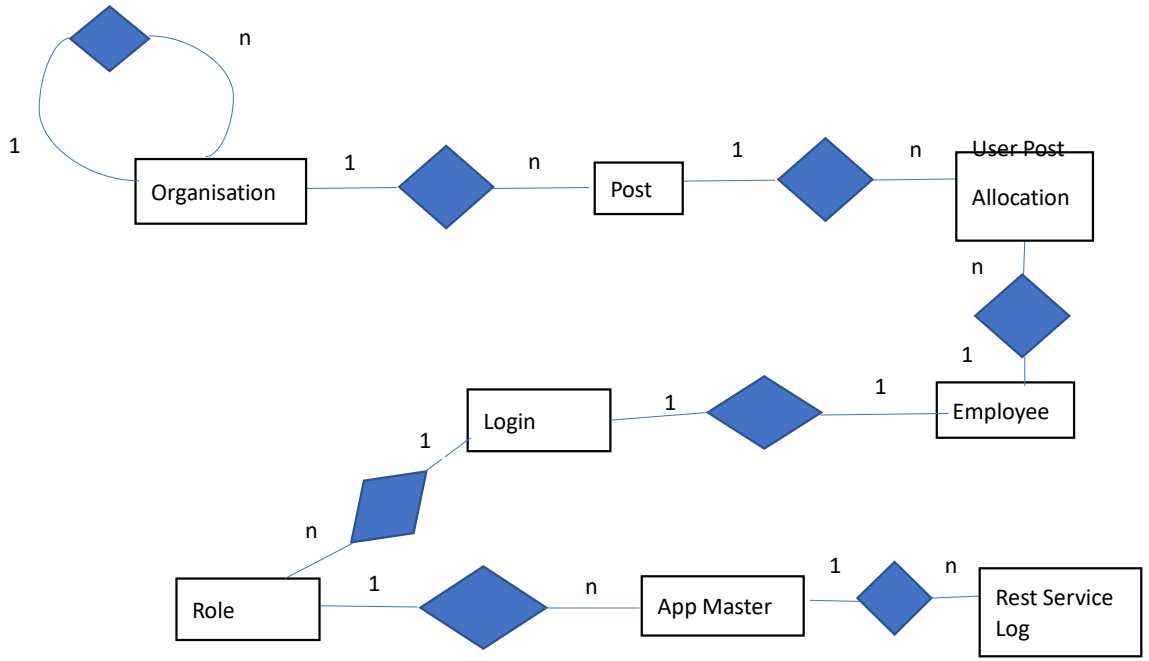
ER 1NF


Organisation
Id Pk
Orgtype, orgtypename
orgName
orgname_hi
abbr_
abbr_hi
parented
stdCode
stdparentcode
Employee
Eid Pk
Desg
Etype
Ecat
State_add
Postid/postname
DepId
InitialName
FullName
Common Address
Permanent address
Login
Id Pk
Password
Username
Eid
Role
Rid Pk
Loginid
applicationId
RoleName
RoleDescription
Userid
App Master
Appid Pk
AppName
AppDescription
AppKeyword
Apptype, ApptypeName
LoginName
appLoginNAme
apploginPassword
appLoginLandingPage
ClientAppid
ApiSharedKey

ER 2NF


Organisation
Orgid /Postid - Partialkeys
Orgtype, orgtypename
orgName
orgname_hi
abbr_
abbr_hi
parentid
parentStdCode
StdCode
PostName
PostCategory
Postname_hi
postShortName
PostPhoneNo1
PostPhoneNo2
PostPhoneNo3
PostPhoneNo4
Login
Id Pk
Password
Username
Eid
Role
Rid Pk
Loginid
applicationId
RoleName
RoleDescription
Userid
App Master
Appid Pk
AppName
AppDescription
AppKeyword
Apptype, ApptypeName
LoginName
appLoginNAme
apploginPassword
appLoginLandingPage
ClientAppid
ApiSharedKey
Employee
EmpId /Postid – Partialkeys
EmployeeFirstName
EmployeeLastName
InitialName
Etype
DesignationId
DesignationName
Common Address
Common Address State
Permanent address State
Email
PhoneNo
MobileNo
PayLevel

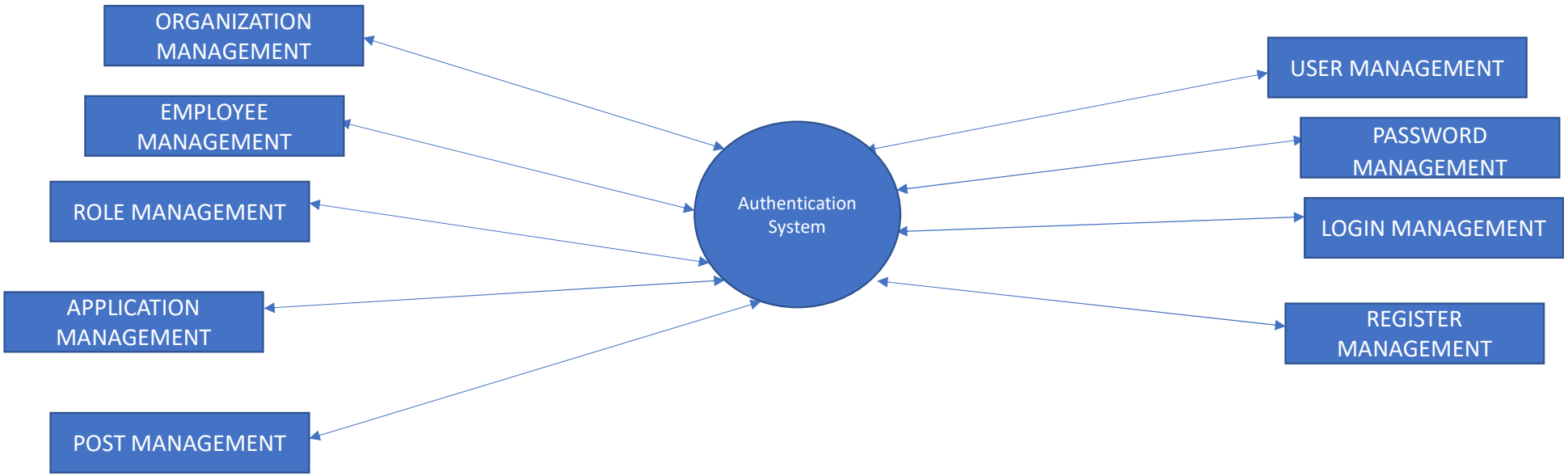
ER 3NF

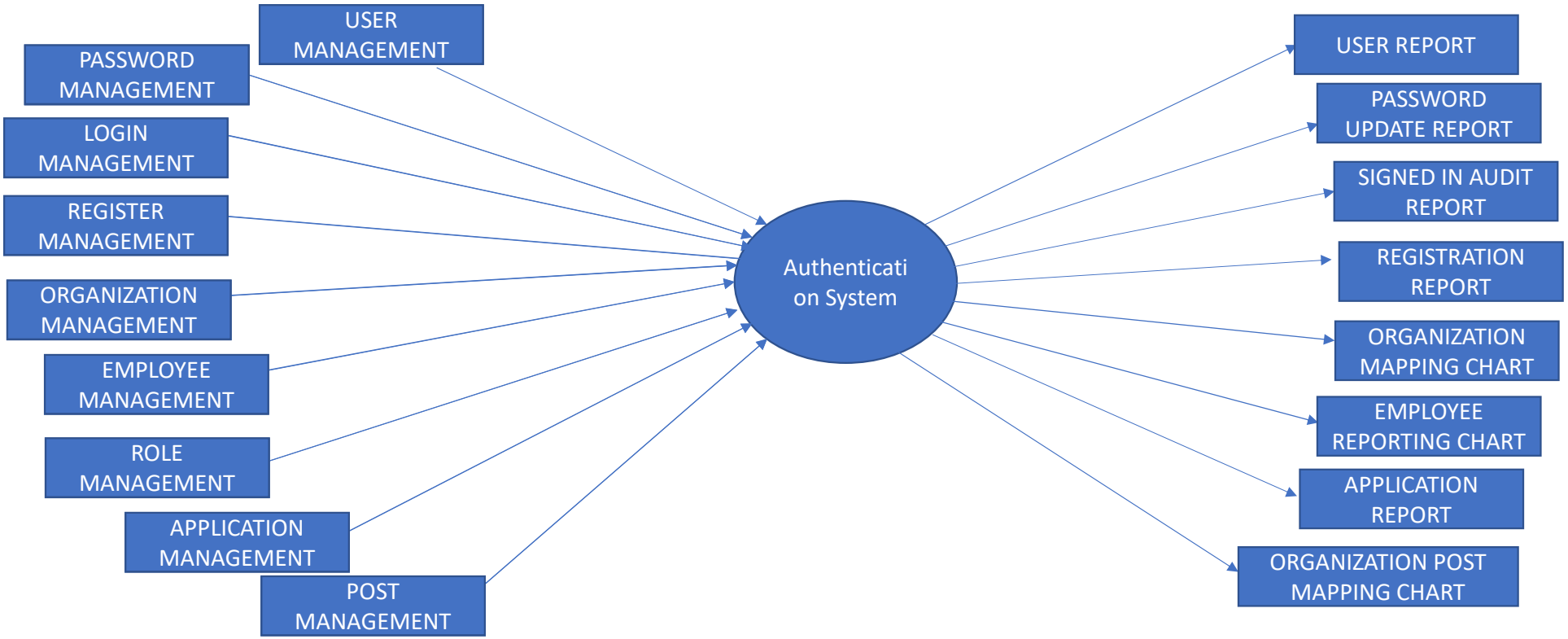

n
1
Organisation
1
n
Post
1
n
User Post
Allocation
n
1
Employee
1
1
Login
1
n
Role
1
n
App Master
1
n
Rest Service
Log

ER-3NF


Organisation
Orgid
Orgtype, orgtypename
orgName
orgname_hi
abbr_
abbr_hi
parentid
parentStdCode
StdCode
Post
Postid
PostName
PostCategory
Postname_hi
postShortName
orgid
PostPhoneNo1
PostPhoneNo2
PostPhoneNo3
PostPhoneNo4
User Post Allocation
UpId
Empid
Postid
Active
VacantDate
JoiningDate
Employee
EmpId
EmployeeFirstName
EmployeeFirstName_hi
EmployeeLastName
EmployeeLastName_hi
InitialName
Emptype
DesignationName
Common Address
Common Address State
Permanent address State
Email
PhoneNo
FaxNo
MobileNo
PayLevel
Empcategory
Hometown
Login
userId Pk
Password
Username
Roleid
Emprefid
Req_passchange
Active
Additional access
Role
Roleid Pk
RoleName
RoleDescription
Privilege
Monitor
active
App Master
Appid Pk
AppName
AppURL
AppLoginPage
LandingPage
ClientAppId
APISharedKey
APISharedId
SecretKey
AppType
AppKeyword
RestServiceLog
RSId
AppId
FunctionName
ResponseString
TimeStamp
Exception
Active
LoginType

DFD(Data Flow Diagram) level 0- CAS




USER MANAGEMENT
PASSWORD MANAGEMENT
LOGIN MANAGEMENT
REGISTER MANAGEMENT
ORGANIZATION MANAGEMENT
EMPLOYEE MANAGEMENT
ROLE MANAGEMENT
APPLICATION MANAGEMENT
POST MANAGEMENT
Authenticati on System
USER REPORT
PASSWORD UPDATE REPORT
SIGNED IN AUDIT REPORT
REGISTRATION REPORT
ORGANIZATION MAPPING CHART
EMPLOYEE REPORTING CHART
APPLICATION REPORT
ORGANIZATION POST MAPPING CHART

Case Study 2- The GGSIPU Leave Management System (GGSIPU-LMS)

- **Problem Statement**
- A web based Leave Management System is required for Guru Gobind Singh Indraprastha University (GGSIPU) where employees should be able to apply for leave online which is processed by the competent authority online along with maintenance of the leave record by the authorized personnel. The leave must be sanctioned as per policy formulated by GGSIPU for different leave types.

Introduction

- The GGSIPU Leave Management System (GGSIPU-LMS) is a software application designed to automate the process of managing leaves of employees of GGSIPU. This system will allow employees to apply for leave, view their leave history, and approve or reject leave requests, if authorized. The personnel department will also have the ability to approve or reject leave requests, if authorized, although they will be able to view the leave status of all employees.

- **Purpose**
- The purpose of the GGSIPU-LMS is to streamline the leave management process and improve communication between employees and personnel departments. The system will provide a common dashboard for managing leave requests of all types, and it will enable automation of the complete leave management process.

System Requirements

- **GGSIPU-LMS requirements in detail**

- **User Roles**

Workflow

- Steps in GGSIPU-LMS workflow
- Security measures:

Use Case Diagram

- Key actors in the GGSIPU-LMS

1. Employee
2. Forwarder/Reporting Personnel
3. Approver/Personnel Department Member
4. System Administrator
5. Accounts department member
6. Monitoring user/Vice Chancellor (VC) office

Use Case Diagram of GGSIPU-LMS

Functional Requirements

Non Functional Requirements

- Non-functional requirements for the GGSIPU-LMS for 5000 employees include:

Case Study 3: Human Resource Management System

(User Requirements)

Example ER Diagram

Example Data Flow Diagram

Employee Maintenance

for the process to maintain employee information.

Example Data Flow Diagram

Job Maintenance

for the process to maintain job information.

Example Data Flow Diagram

Job Assignment Maintenance

for the process to maintain job assignment information.

Example Data Flow Diagram

Location Reporting

for the process to report location information.

Consider the problem of railway reservation system and design the following:
(i) Problem statement
(ii) Use case diagram
(iii) Use cases.

Discussion Question

Consider the following requirement: “The system shall have 3-tiers: a web-based presentation tier, logic tier, and data tier that uses a relational database.” Is this an acceptable requirement?

- **ANSWER**: Requirements should focus on WHAT is required to be solved by the system and not the HOW part: specifying that the system should consist of 3-tiers is about HOW aspects of the system.
- Since the requirement talks about the HOW part, this is not an acceptable requirement.

- In airline tracking system, the system shall assign a unique PNR number to each booking. **(Functional Req/ Non-functional Req)**

- FastTag in electronic Toll collection system assign UPI Id for making toll payments from customers linked prepaid or saving account. **(Functional Req/ Non-functional Req)**

- In Airline Tracking System

"Given a PNR number as input, the system should display the status of the flight within 3 seconds to the user (performance requirement).
(Functional Req/ Non-functional Req)

"The System shall protect against unauthorised addition or deletion of PNR number." (Security Requirement)

(Functional Req/ Non-functional Req)

COCOMO MODEL

- A project size of 200 KLOC is to be developed. Software development team has average experience on similar type of projects. The project schedule is not very tight. Calculate the effort, development time, average staff size and productivity of the project.

$$E = a_b (KLOC)^{b_b}$$

$$D = c_b (E)^{d_b}$$

$$(SS) = \frac{E}{D} Persons$$

$$(P) = \frac{KLOC}{E} KLOC / PM$$

E = 1133.12 PM

D = 29.3 P\M

Software Project	a_b	b_b	c_b	d_b
Organic	2.4	1.05	2.5	0.38
Semidetached	3.0	1.12	2.5	0.35
Embedded	3.6	1.20	2.5	0.32

Table: Basic COCOMO coefficients

A simple stand – alone software utility is to be developed in 'C' programming by a team of software experts for a computer running Linux and the overall size of this software is estimated to be 20,000 lines of code. Considering (a, b) = (2.4, 1.05) as multiplicative and exponention factor for the basic COCOMO effort estimation equation and (c, d) = (2.5, 0.38) as multiplicative and exponention factor for the basic COCOMO development time estimation equation, approximately how long does the software project take to complete ?