College ERP(Enterprise Resource Planning) Management System

A CS814 Course Project Report

Submitted by,

Yash Madwanna (202IS017)
Rohan Rangari (202CS023)

Department of Computer Science and Engineering
National Institute of Technology Karnataka
P.O. Srinivasnagar, Surathkal, Mangalore-575 025
Karnataka, India
January 2021

Table Of Contents

Introduction:

College ERP Management System:

College ERP management system is a solution for managing various facilities provided by the department to students ,faculties, and admin. Managing various kinds of users at a single place is relatively simpler than managing each user individually. The management here means giving various permissions to the users according to the permissions allowed for that particular user.

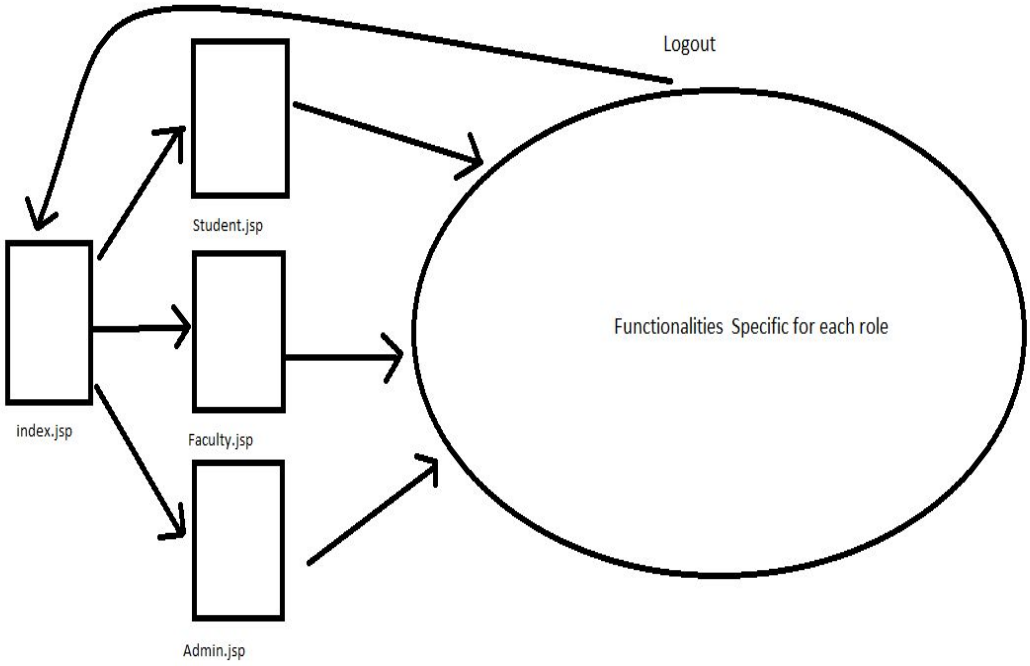
Some of the advantages of this application is

1. Reduction in manual work
2. Data remains synchronous.
3. Availability
4. Customization is possible.

Architecture Of Application:

The College ERP project currently manages data for the Computer Science and Engineering Department only.

The overview of architecture is shown below:

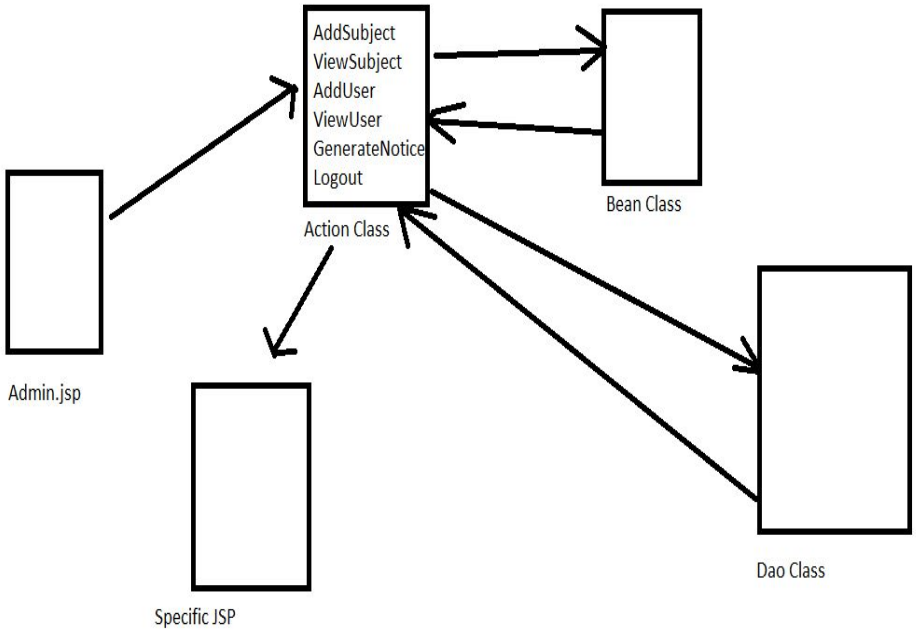


(Figure 1. Flow of Application)

The index.jsp is the home page in this application. Any user can login into this application provided that user is registered. After successful login users get a screen which is specified for their role.For Example. If the user is Admin then they will get an admin panel, if the user is faculty then they will get faculty screen and student will get student screen. The redirection is done at runtime based on the role which is mapped with the user.

Admin:
Admin is responsible for overall management of the system. Only Admin can give credentials to new users and also role assignments .

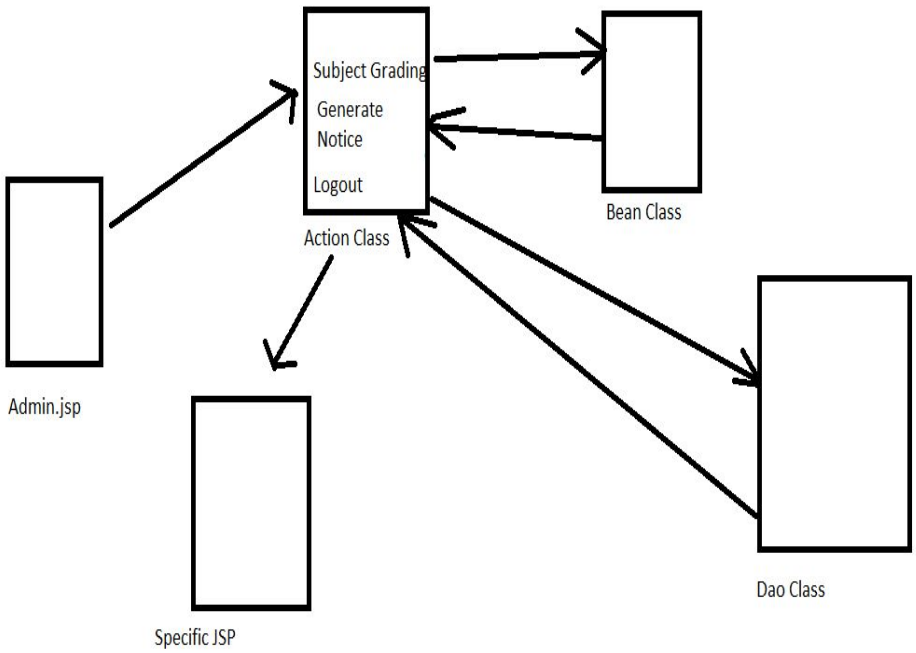
Functionalities provided here are :
AddSubject : This is used to add new subjects into the database.
View Subject : It is used to View all the subjects which are present into database
Add User : It is used to add a new User into the system.
View User : It is used to view all the users info which are present into the system.
Generate Notice : It is used to generate notices .
Logout: It is used to logout from the system and invalidate sessions.



(Figure 2. Admin.jsp)

Faculty:
The Faculty is responsible for grading of students and also for notice generation if permission is granted by the admin.

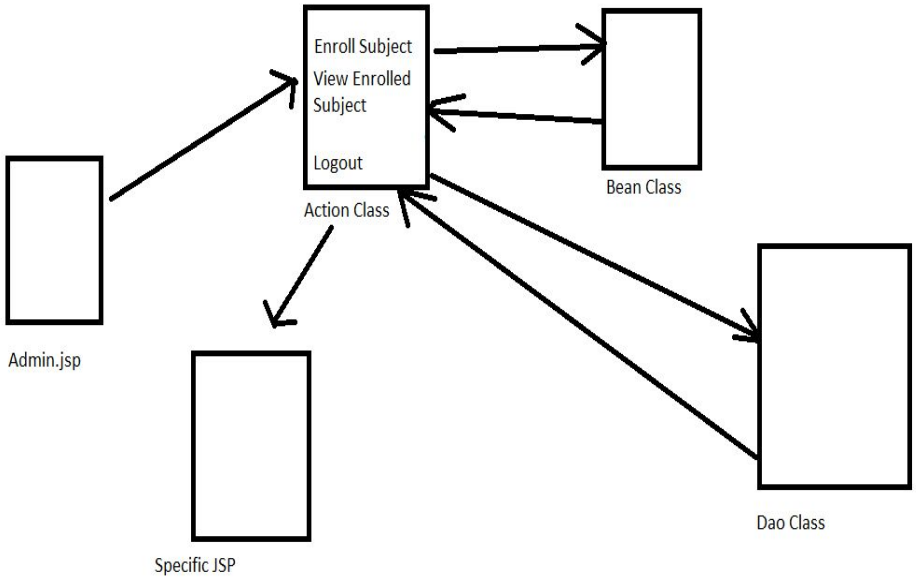
Functionalities provided here are:
Subject grading : Faculty can add students' grades for the subjects which are assigned to them.
Notice Generation : Faculty can generate notices if permission is given by admin.
Logout: It is used to logout from the system and invalidate session.



(Figure 3. Faculty.jsp)

Students:
Students can see activities related to their academics such as enrolling into subjects and also can view enrolled subjects.

Functionalities provided here are:
Enroll Subject: Students can enroll into new subjects which are available for them.
View Enrolled Subject: Students can view their enrolled subjects.
Logout: It is used to logout from the system and invalidate session.



(Figure 4. Student.jsp)

Authorization

Need of RBAC based Authorization:

A Role-Based Access Control is a method of restricting access within an organization based upon the role of the respective user. A user's role within the organization decides what kind of permissions he/she possesses. In role-based access control model roles are based upon several factors, including authorization, responsibility and job competency. As such organizations can designate whether the user is an end-user, the administrator, or the special user, etc. Limiting the access to the system is important as many users might not be permanent, or permitting access to the third parties, like customers, and vendors, makes it difficult for managing access effectively. If organizations use the RBAC model, they are better able to secure the sensitive information, data, and critical applications. Organizations can control access to the data, information depending upon the role of the user. So only privileged users can access the sensitive information.

Benefits of using RBAC:

1. *Improving Operational Efficiency:* With RBAC, companies can decrease the need for paperwork and password changes when they hire new employees or switch the roles of existing employees. RBAC lets organizations quickly add and change roles, as well as implement them across platforms, operating systems (OSes) and applications.
2. *Giving administrators increased visibility:* RBAC gives network administrators and managers more visibility and oversight into the business, while also guaranteeing that authorized users and guests on the system are only given access to what they need to do their jobs.
3. *Reducing costs:* By not allowing user access to certain processes and applications, companies may conserve or more cost-effectively use resources, such as network bandwidth, memory and storage.

Components of RBAC present in application: In our application, we have used password based authentication (log-in) to access the system. We have 3 types of users 1) Student 2) Teacher 3) Administrator. It also means we have 3 roles in our RBAC based application as mentioned above. Each user after successful login has their own session. We also created a permission 'generate notice' every user in the system by default possesses this permission. But the administrator can change who can access this permission.

The user student has access only to functionalities like Enroll Subject and View Subject, etc. The user teacher has access to functionalities like Subject Grading and Notice Generation, etc. The administrator has access to functionalities like Add User, View User, Add Subject, View Subject, Generate Notice, etc. So we can see we separated permissions and functionalities based upon the role of the user.

Components of Administrative Model:

The administrator can add a new subject to the system, new user to the system, invoke or revoke notice generation permission to different users.

Implementation of Authorization:

We have used log-in based authorization. Each user will log-in to the system using email id and password. An email is assigned to the role of user to it and an email id is unique. Depending upon the role, after successful login the user will be granted appropriate privileges according to its role.

Conclusion :

RBAC policy is useful when we have a very large number of users associated with ‘n’ roles.

In the end, we can say that we have successfully demonstrated the RBAC policy in our college ERP application. We have identified users by their respective roles, separated their functionalities, permissions according to their role. The RBAC policy implementation in our application helped us to separate student and teacher policies, permissions, etc from that of highly privileged administrator policies, permissions. It improved the operational efficiency from an administrator's perspective. But also reduced the operational cost of the organization otherwise 3 different system should have to be maintained and synchronization between 3 of them would be a quite difficult task.

References

- R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, "Role-based access control models," in Computer, vol. 29, no. 2, pp. 38-47, Feb. 1996, doi: 10.1109/2.485845.
- https://dev.mysql.com/doc/refman/en/
- https://www.w3schools.com/html/html_scripts.asp