Library Management System with Role Based Access Control(RBAC) Authorization/Authentication policy

CS814 Course Project Report

Submitted by:

Abhilash Ghope 202CS001

Takesh Katlam 202CS032

Department of Computer Science and Engineering
National Institute of Technology Karnataka P.O. Srinivasnagar
Surathkal, Mangalore-575025, Karnataka India

January 2021

Contents:

Introduction:

The Library Management System with Role Based Access Control(RBAC) Authorization / Authentication policy that uses to maintain the record of the library. It contains work like the number of available books in the library, the number of books are issued or returning or renewing a book or late fine charge record, etc. Library Management Systems is web application that helps to maintain a database that is useful to enter new user & record books borrowed by the staff, with the respective submission dates. Moreover, it also reduces the manual record burden of the librarian.

Library management system allows the librarian to maintain library resources in a more operative manner that will help to save their time. It is also convenient for the librarian to manage the process of authorizations and authentications. Library management system is also useful for students as well as a librarian to keep the constant track of the availability of all books in a store.

Authorization:

Need of RBAC based authorization:-

In this Library Management System the RBAC lets users have access rights only to the information they need to do their jobs and prevents them from accessing information that doesn't pertain to them. In the role-based access control data model, roles are based on several factors, including authorization, responsibility and job competency. This system also have the components like admin,library staff, users. So,there is necessory to implement the aauthorization and authentication system to control the access of every members.

Components of RBAC present in this Application:-

User-role={user, staff, admin}

Role-permission={read, add_user, delete_user, update_user_info, }

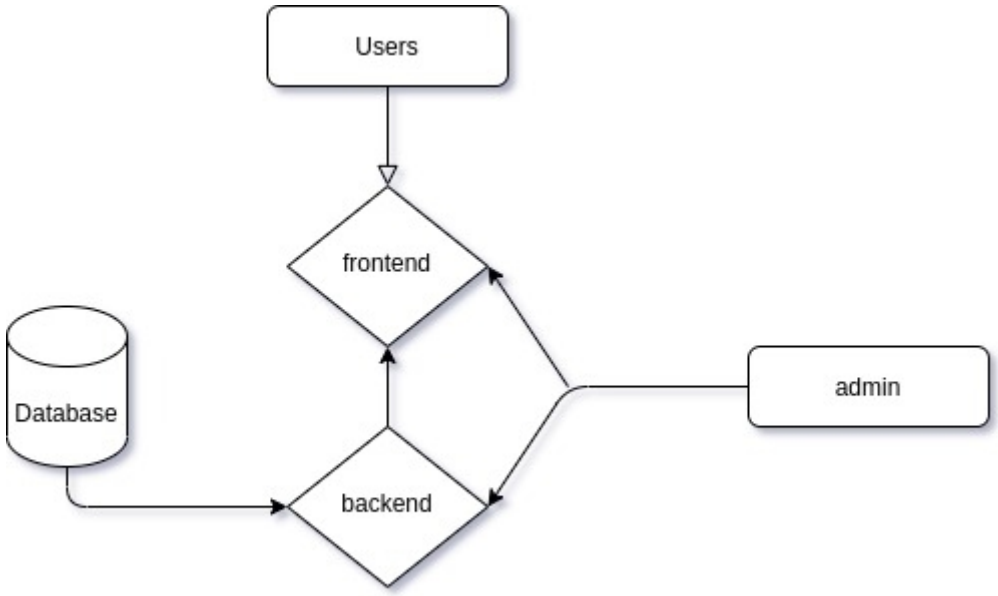
Components of administrative model present in this Application:-

User-role={user, staff, admin}

Role-permission={read, add_user, delete_user, update_user_info, }

Role-Assignment={user_role, staff_role, admin_role, }

Data Flow Diagram:



Conclusion:

- RBAC is used to simplify security policy administration.
- RBAC is sn open-ended technology, which ranges from very simple to fairly sophisticated.
- RBAC continues to be an evolving technology.
- However, RBAC is also more powerful and flexible than using only function security.

References:

- **N IEZETTE , M. AND S TEVENNE , J. 1992. An efficient symbolic representation of periodic time. In Proceedings of the First International Conference on Information and Knowledge Management.**
- **N YANCHAMA , M. AND O SBORN , S. 1999. The role graph model and conflict of interest. ACM Trans. Inf. Syst. Sec. 2, 1, 3–33.**
- **O SBORN , S. (ED .) 2000. Proceedings of the Fifth ACM Workshop on Role-Based Access Control(Berlin).**
- **O SBORN , S., S ANDHU , R., AND M UNAWER , Q. 2000. Configuring role-based access control to enforcemandatory and discretionary access control policies. ACM Trans. Inf. Syst. Sec. 3, 2, 85–106.**
- **S ANDHU , R. 1991. Separation of duties in computerized information systems. In DatabaseSecurity IV: Status and Prospects, North Holland, Amsterdam, the Netherlands, 179–189.**
- **S ANDHU , R. (ED .) 1995. Proceedings of the First ACM Workshop on Role-Based Access Control(Fairfax, Va.).**