REPORT ON

BANKING SYSTEM WEB APPLICATION
USING RBAC POLICY

UNDER THE GUIDANCE OF
Dr. Mahendra Pratap Singh

SUBMITTED BY
Dheeraj Kumar Srivastava (Roll no. 202CS006)
Vinayak Prakashan Choyyan (Roll no. 202CS033)

CS814 COURSE PROJECT

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

Contents

List of Figures

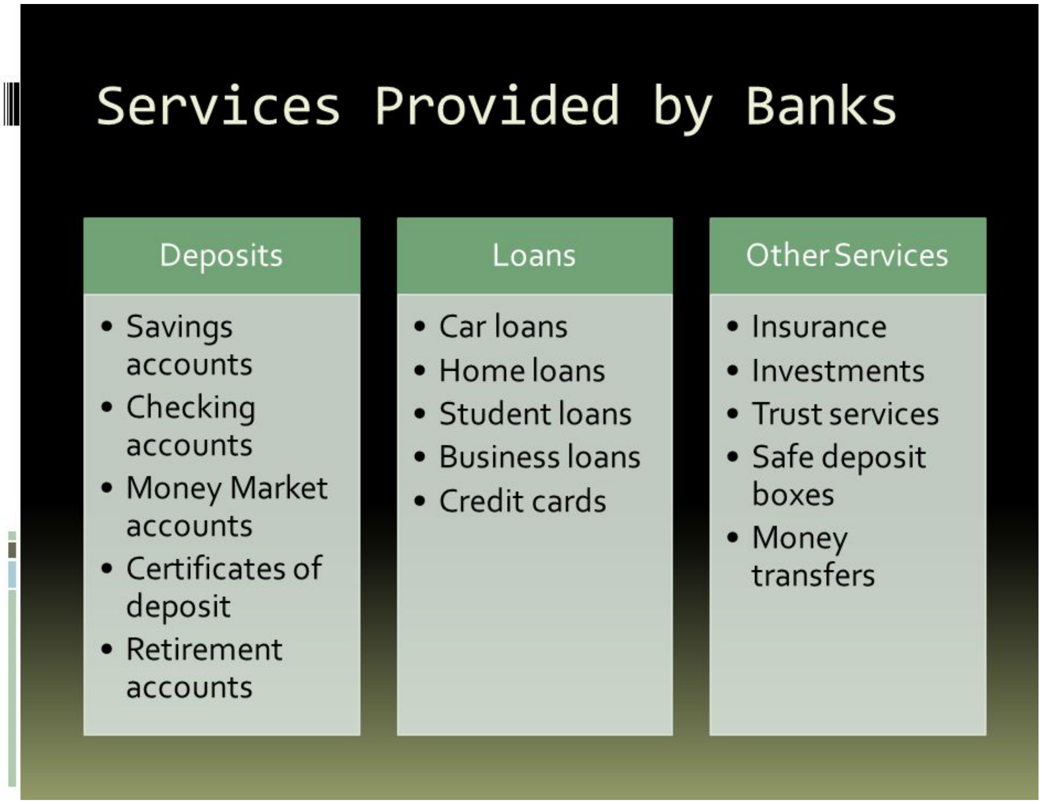
1 INTRODUCTION

Banking system is an interface for varous financial services.It provides services such as saving money in the account, debit, credit etc.Banking system being directly connected to financial services require a very high level of security for its proper and correct functioning.Later in the report the most used RBAC policy is discussed that has been used in this project on for proper access control over the etire banking system implemented.

The project is aimed to implement the basic model on Banking System with various services like debit,credit,transfer etc.For developing the application php, html, css are used for implementing the basic model.In the project Mysql database is used for data storage for various purpose.For Mysql and apache server , Xampp software is used which provides these tools in one singke package.

Banking System requires authentication and access control mechanism for accesibilty of its various access rights or permissions.for intance normal user should have accessibilty like debit theri money aur transfer money from their account to any other account.Similarily Employee have more access rights that they can perform like updating users information on user request ,credit amount into the user account after receiving and verifying the amount of money,view users or customer's information.Also there should be an Administrative user that have priviledges like changing authentications for employee as well as employee.One can also think of a super or senior Admin that have the higher power over all the administrator in case of large organisation.

There are many other constraint to be taken into the mind while developing Banking System.For instance Employee of the bank have all the permission to view customer's information but allowing employee to access all the customer's(user's) information is not required as well as can cause certain threats to the security.Thus Banking System should be developed keeping all these constraint into mind. That means permisison should also have certain boundation over them.



Services Provided by Banks

Deposits	Loans	Other Services
• Savings accounts	• Car loans	• Insurance
• Checking accounts	• Home loans	• Investments
• Money Market accounts	• Student loans	• Trust services
• Certificates of deposit	• Business loans	• Safe deposit boxes
• Retirement accounts	• Credit cards	• Money transfers

Figure 1: BANKING SYSTEM SERVICES

2 AUTHORISATION

In the model of the presented Banking System environment we have implemented RBAC Policy for access control.Before going into how it is implemented in our banking system application lets take a view as how RBAC Policy work.

2.1 RBAC(Role Based Access Control)Policy

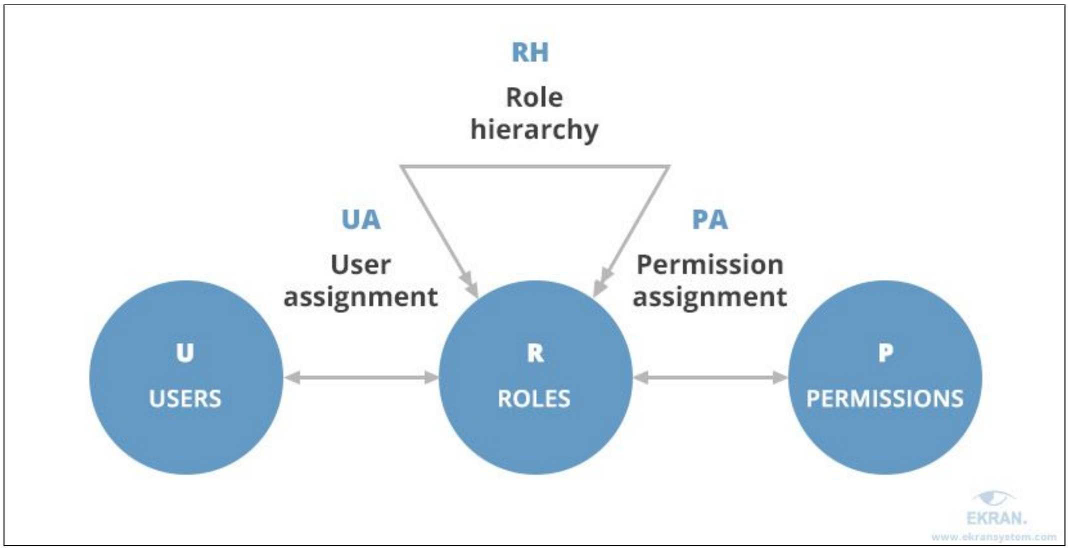


Figure 2: RBAC POLICY MODEL

In RBAC Policy,each member that uses the system are assigned role/s and for each role we have sets of permission.So the member (Normal customer, employee) can have certain sets of access permission allowed to them based on the role they have.So on RBAC POLCY access control is based on funtionality not the idenity of any user.

In RBAC, this role inclusion in the access control gives an advantage to the model functionality.For eg. let say Vinayak was working as an employee in the SBI DELHI but was transfered to some other place and some other person say Aman is given that vacant post. Now since in the Banking Authorisation we have implemented RBAC Policy, we can simply give the role ”employee” to Aman to acces same as that of Vinayak.Now Aman can work as employee and can have all permission associated with the role ”employee”.

Banking System is one of the crucial place where proper authentication for data and resource accessibity is very important.Since for a banking system number of users are very large so using an access control policy such as DAC (using ACM)is not practical

2.2 CONVENTION

- U = set of users
- R = set of Roles
- P = set of all Permission

- UA or URA = user role assignment.(many to many relation as a single user can have more then one role and a role can be given to more then one user
- PA or PRA = permission role assignment(many to many relation as one role can have more then one permission and one permission can be given to more than one role.

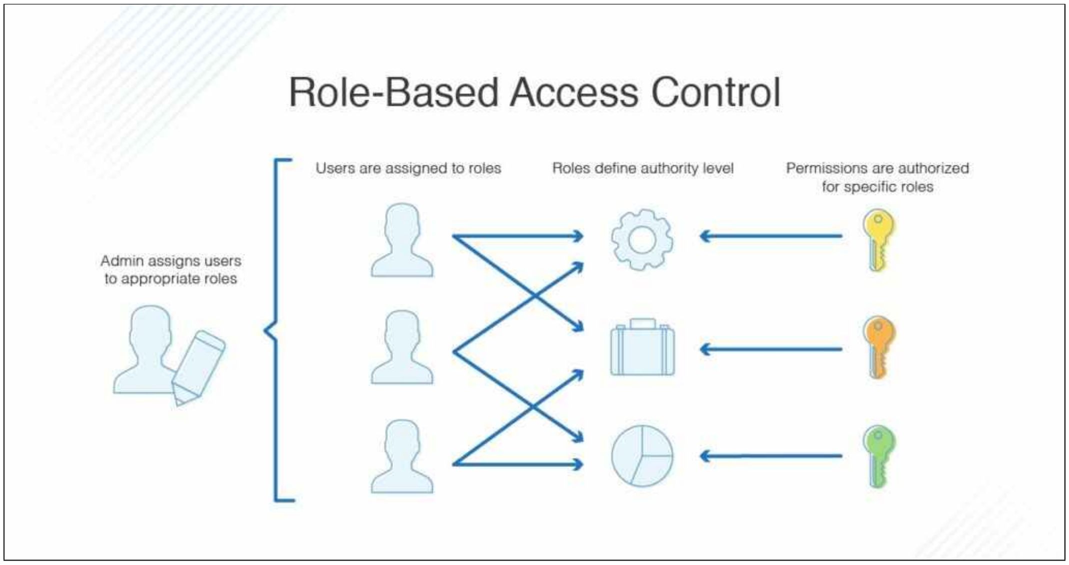

Role-Based Access Control
Admin assigns users to appropriate roles
Users are assigned to roles
Roles define authority level
Permissions are authorized for specific roles

Figure 3: RBAC POLICY MODEL-II

2.3 TERMINOLOGY

- Role Assignment-A subject is associated with a role.
- Role Authorisation-All roles have set of permission associated with it.
- Permission Authorisation-Any subject can have permissions based on their role.

2.4 DATABASE IMPLEMENTATION

For Implementing RBAC in our Banking System Application, we have used 6 tables (5 related to RBAC and 1 for all details of the customer).These tables are

- Users=Representing users(userId and Password)
- Roles=Representing roles(roleId and rolename)
- Permissions=Representing permissions(perId and permission)
- UR=User role assignment (userId and roleId)
- PR=Permision role assignment (roleId and perId)

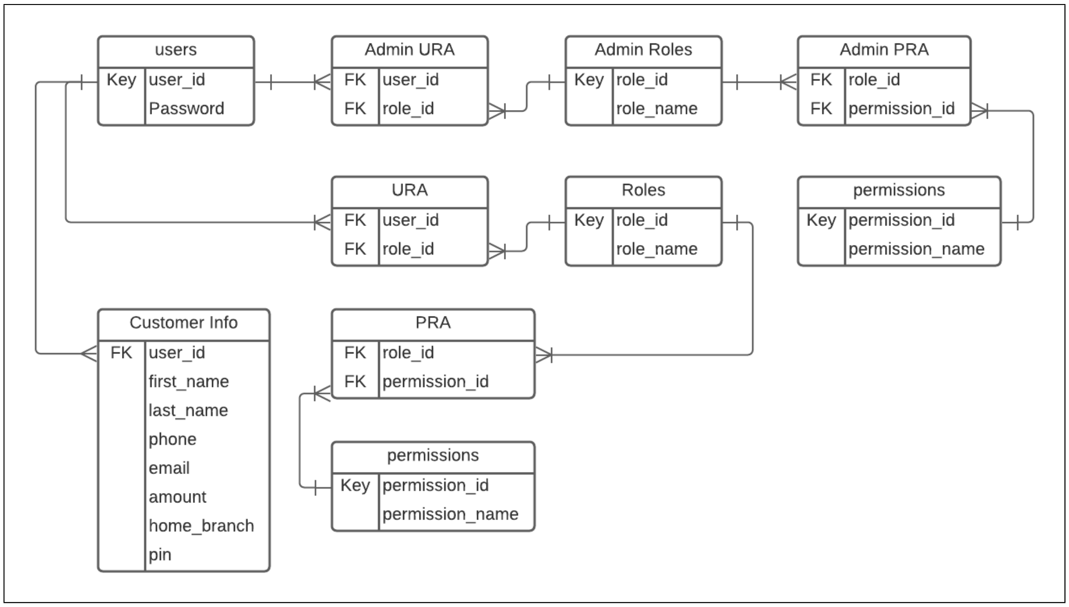


Figure 4: SCHEMA DIAGRAM FOR DATABASE TABLES

The user table contains set of users(userId or username) and password for authentication purpose.After authentication using UA (UR) table in database is used to find the roles for that user.Afterwards there is a table for roles(roleId and rolename) for all the roles created.After using UA , the role associated with the user is used to find the set of permission associated with the user using PR table (PR) in the databases.All these things occure at backend.So just after the authentication on login, user will be able to see set of permission associated with him which that user can use to access features , data and accessibility of system.

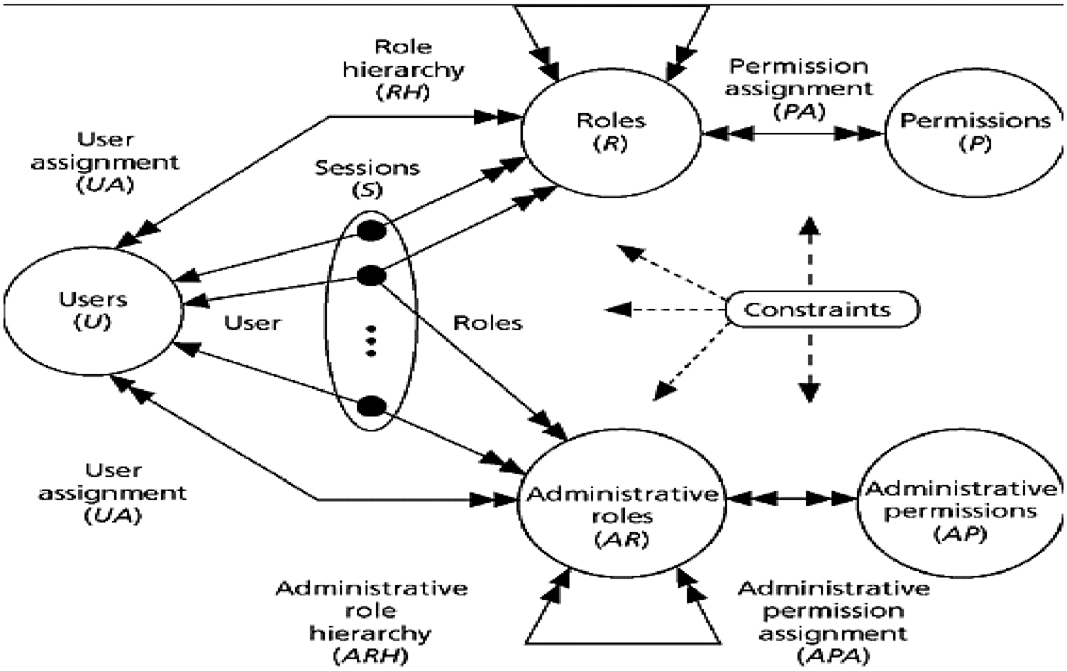

Role hierarchy (RH)
User assignment (UA)
Sessions (S)
Roles (R)
Permission assignment (PA)
Permissions (P)
Users (U)
User
Roles
Constraints
User assignment (UA)
Administrative roles (AR)
Administrative permissions (AP)
Administrative role hierarchy (ARH)
Administrative permission assignment (APA)

Figure 5: RBAC WITH ARBAC

Administration using ARBAC is also implemented with some functionality.
It uses the following tables in the database

- Users=same for normal user and admin where admin and there password are stored as nomal user and employee.
- Admin role=roles of admin
- Admin permission = set of all permission related to admins.
- AR=Admin role assignment
- AP=Admin permission assignment

These database tables associated with admin works the same way for finding admin to role to permission that an admin can have.

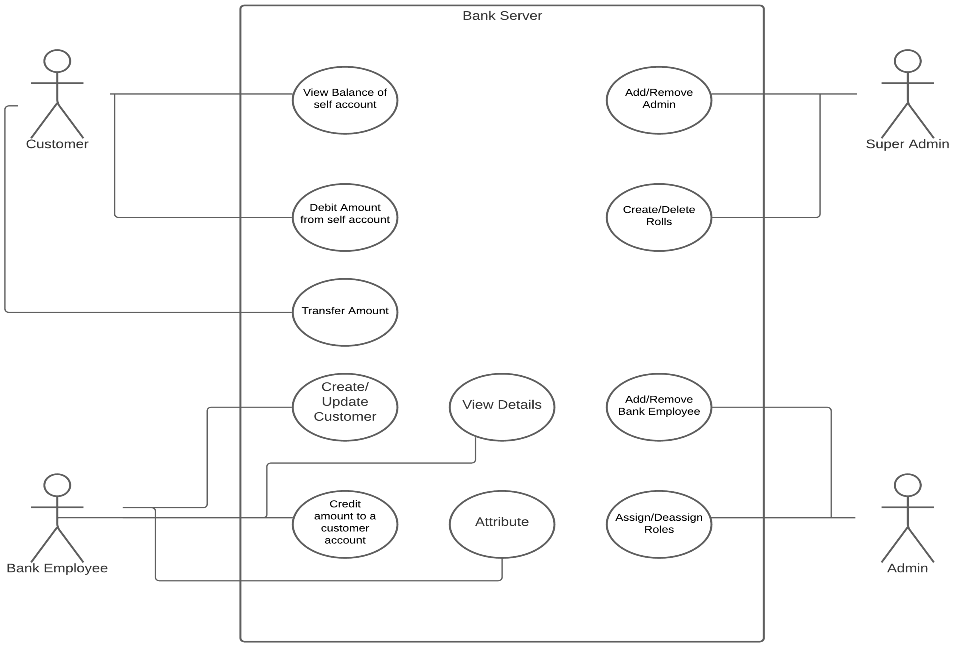


Figure 6: USE CASE DIADRAM

3 CONCLUSION

Banking System is one of the crucial place where proper authentication for data and resource accessibity is very important.Since for a banking system number of users are very large so using an access control policy such as DAC (using ACM)is not practical.Also since Banking system is very dynamic in terms of users, employees and accounts it is very difficult if we are using an access control method which is defined on per user level definition which is again very much inpractical.

Policies like RBAC implemented in Banking System are of atmost use in these scenarios.As RBAC policy defines access per functionality rather then per idenitity implementation, it can implemented easily in such dynamic environment providing access control based on roles a user is assigned.User having the particular role can access all the permission associated with that role.

Here administration is a problem,which can be solved using ARBAC policy that uses the same concept of RBAC to administrate RBAC.Thus we RBAC rules itself in the form of ARBAC can be used for administration.

4 REFERENCES

1].Role-Based Access Control Models by Ravi S. Sandhu, George Mason University and SETA Corporation

2].The ARBAC97 Model for Role-Based Administration of Roles,Ravi sandhu,Venkat Bhamidipati,and Qamar Munawer

3]S ANDHU , R. AND B HAMIDIPATI , V. 1997. The URA97 model for role-based administration of user-role assignment. In Database Security XI: Status and Prospect, T. Y. Lin and X. Qian, Eds. Elsevier North-Holland, Inc., Amsterdam, The Netherlands.

4]S ANDHU , R. 1997. Roles versus groups. In Proceedings of the 2nd ACM Workshop on Role-Based Access Control (Fairfax, VA, Nov. 6-7). ACM Press, New York, NY.

5]S ANDHU , R. S. 1992. The typed access matrix model. In Proceedings of the ACM Symposium on Research in Security and Privacy (Oakland, CA, May). 122–136