system design document

System Functions Outline

Our goal is to build web application for access review. The review should provide all the functions below:

- Visualize access control list to facilitate permission review and audit. The userlist and their permissions of these services are supplied in csv file format. We need to parse these data, store it in the backend database and display content in a good manner.
- Provide authentication and session management for different roles. When users log into the system, the dashboard should display different content based on user's role.
- An administrator is needed for the system. The system should provide interfaces for admin to manage the whole system. An admin can perform operations like create app, upload permission file, assign permission for managers and auditors and so on.
- The system should provide a way to generate reports after review process is completed. PDF is a widely used format for report, so we plan to implement a pdf generator for the system to dynamically output report.
- Session management and authentication are still required for the system for security reason.

Roles Outline

In our apps, there are five kinds of entities Admin, Auditor, Manager, Users and Applications.

- Admin is the one that controls the whole app, he can decide who is the manager of what application, and who is the auditor. If the identity of someone is changed, the admin would change its permission in the application immediately. There is only one admin in the application
- User means the normal user in the app that do not have any privilege to the applications and cannot change the userlist. They can only review the applications that assigned to them.
- Auditor is the one that audit all the applications, he can verify the process and make sure everything is going right. Auditor can only view the access permissions for all services.
- Manager is the one that reviews applications assigned to him, he can change the permission if he/she finds something is not right in the list. And he can approve or deny the review list.

- Application means the services involved in the company, for example: AWS and Rightscale. When users log into the system, the dashboard would display the applications that are related to themselves.

Relation

There are several relations in this system:

- App-User-Permission

This is the real access control list. Given an app and a user id, the matrix will show which permission the user has for this application.

All the access review process are related with this relation table and it is the most important part of the project.

- App-Manager

This relation shows the permission of managers. This is assigned by administrator and performs the access control for managers of the system.

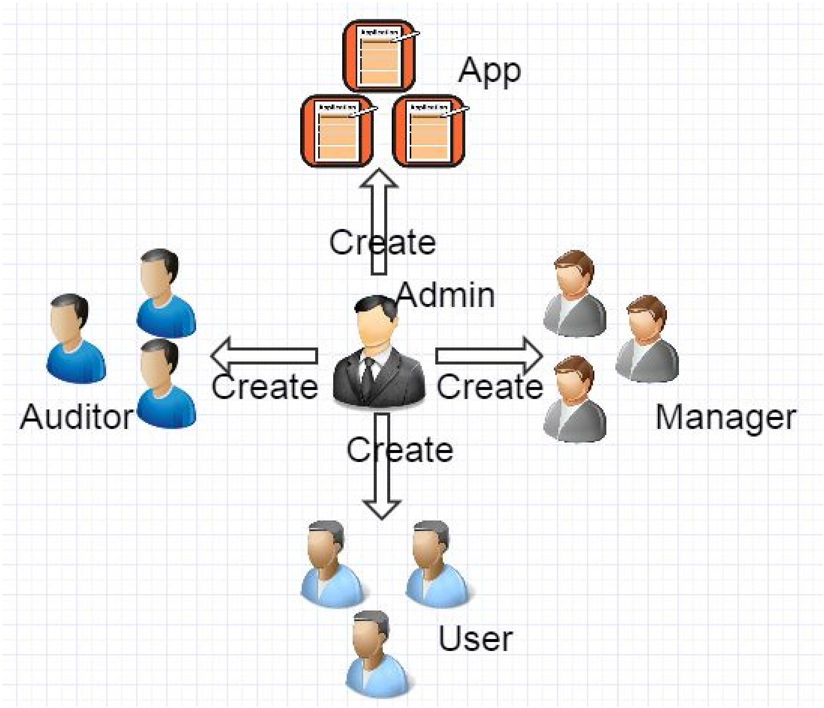
- App-Auditor

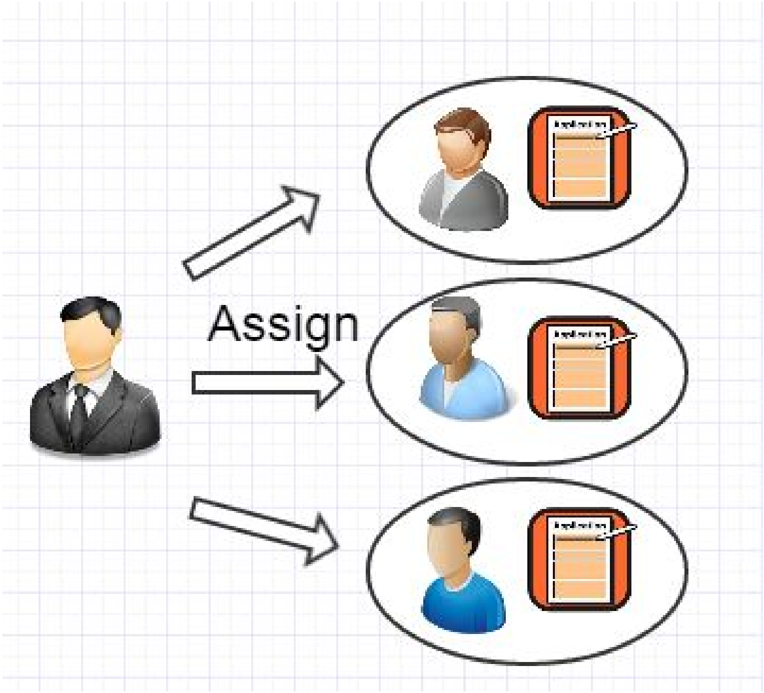
This relation shows the permission of auditors. This is assigned by administrator and performs the access control for auditors of the system.

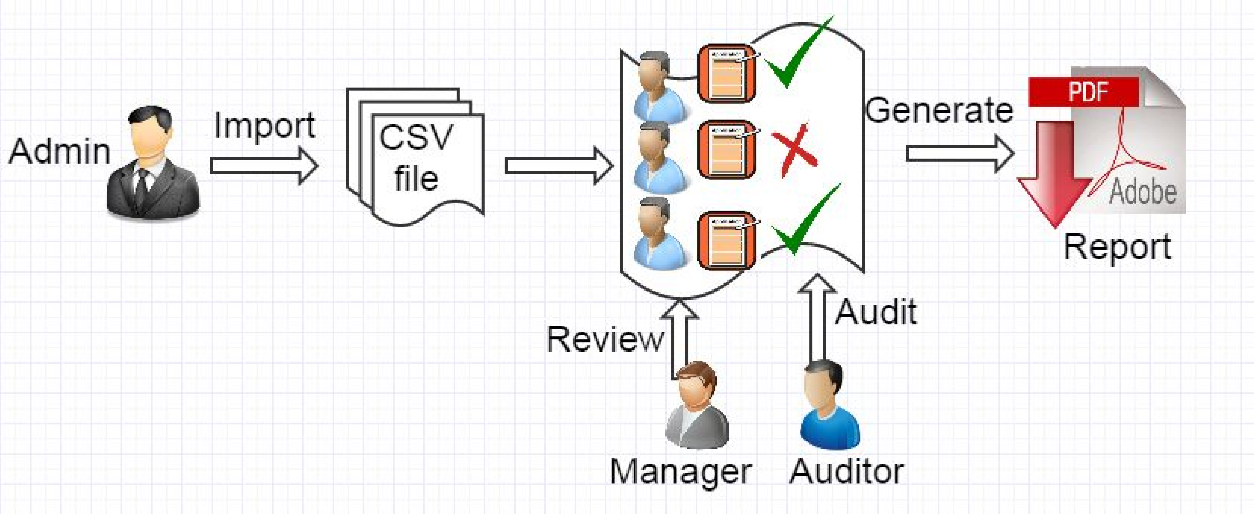
Data Extraction

To get the real access control matrix, we have to parse our raw data to a data structure which can be stored in the back end database.

For this part, we build data extraction module to parse csv files supplied by our customer and build a user-app-permission matrix and store it in the database.


App
Create
Admin
Create
Create
Auditor
Manager
Create
User


Assign


Admin
Import
CSV file
Generate
PDF
Adobe
Report
Review
Audit
Manager
Auditor