第七章系统安全和权限设计

7.1系统安全设计原则

由于在网络环境下，任何用户对任何资源包括硬件和软件资源的共享，所以必须通过制定相应的安全策略来防止非法访问者访问数据资源，对数据资源的存储以及传输进行安全性保护。

7.1.1标识与确认信息

用户在访问小程序资源时，必须得到系统的身份认证以及身份标识，如学号、姓名、系别、专业等。当用户信息与数据库中的学生信息一致时，才能获准访问小程序。

7.1.2授权

对用户授予访问小程序页面资源的权限，例如打卡，浏览排行榜、查看个人信息，日历图的签到补签等功能。

7.2系统级安全

系统级安全主要体现系统软件平台的安全设置上。

7.2.1操作系统平台的安全管理

保证学生用户对数据库的数据文件不能有可写、可删除的权限，以保证数据库的数据信息不会被随意篡改导致其他用户信息出错。

7.2.2数据库系统的安全管理

数据库系统是整个系统的核心，是所有业务管理数据以及清算数据等数据存放的中心。数据库的安全直接关系到整个系统的安全。通过区分不同的访问者、不同的访问类型和不同的数据对象，进行分别对待而获得的数据库安全保密设计，考虑如下：

（1）数据库由专门数据库管理员对数据库操作。管理员权限最大，可以控制所有数据，同时，数据库的密码应由专人负责，密码应该定期变换。

（2）小程序连接数据库的用户绝对不能使用及修改数据库，必须对其进行严格的权限管理，控制对数据库中每个对象的读写权限。

（3）利用数据库的审计功能，以对用户的某些操作进行记录。充分使用视图以及存储过程，保护基础数据表。

7.3应用级安全

针对本小程序，我们在考虑其应用级安全时，主要针对系统的用户授权及安全访问控制

7.3.1用户授权及安全访问控制

用户只有一种进行学生认证成功的学生用户。

通过学生认证的学生用户在不违背系统规则情况下可以使用小程序页面的所有功能。

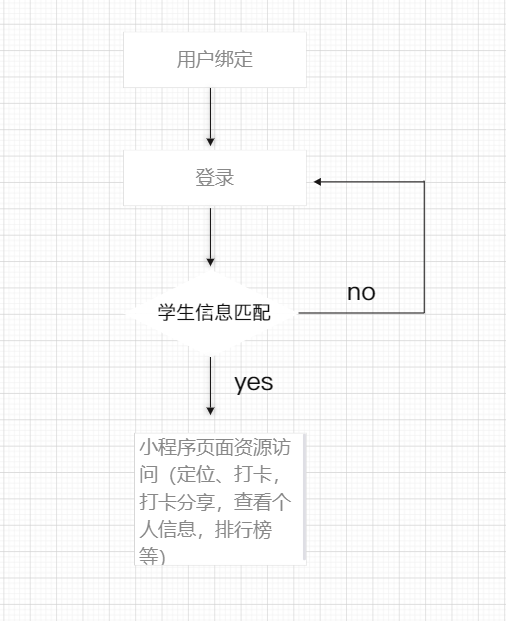
对系统的使用范围包括一个时间范围：及早上八点到晚上九点期间才能使用系统，其他时间系统都处于停止服务状态。

·用户认证

使用小程序的主体在进行身份认证时，需要提供学生信息和身份信息。只有正确符合学生和身份信息的用户才会被允许登录

·用户授权

给学生用户授予访问资源的权限：



7.4权限管理

权限管理是用户进行系统权限划分和设置的平台，按照管理的层次可划分为

两个层面进行管理，管理员和学生用户。

7.4.1管理员

管理员权限最大，可以控制数据库的修改及使用还有小程序的所有数据。

7.4.2学生用户

学生用户权限低于管理员，没有操作数据库的权限，只能使用小程序已有的定位，打卡，分享等功能模块。