《系统设计说明书》

网益云

成员： 岳嘉宁、连书缘、胡启华、徐源、白耿龙、李冰鑫、林钊宁、林鸿、吴少冰、余立

目录

1. 引言

1.1编写目的

本设计说明书文档包括该项目的建设背景、功能、权限设计、安全设计等的描述，用于指导该项目的开发与部署，同时，作为该项目的重要技术资料，作为系统未来维护或拓展的参考。本文档的阅读者为本系统的设计、开发人员、接口系统的开发人员、系统维护人员。

1.2 背景

a.软件系统名称：Antidote
b.提出者：岳嘉宁
c.开发者：网益云团队
d.用户：全体注册成功的消费者

1.3 实现功能

a.文章浏览，让用户能再文章中找到心灵上的安慰。
b.精品电台和舒缓音乐帮助用户更好的方式。
c.心理测试，为用户提供心理测试，帮组用户。
d.心理咨询预约，给用户提供预约平台。

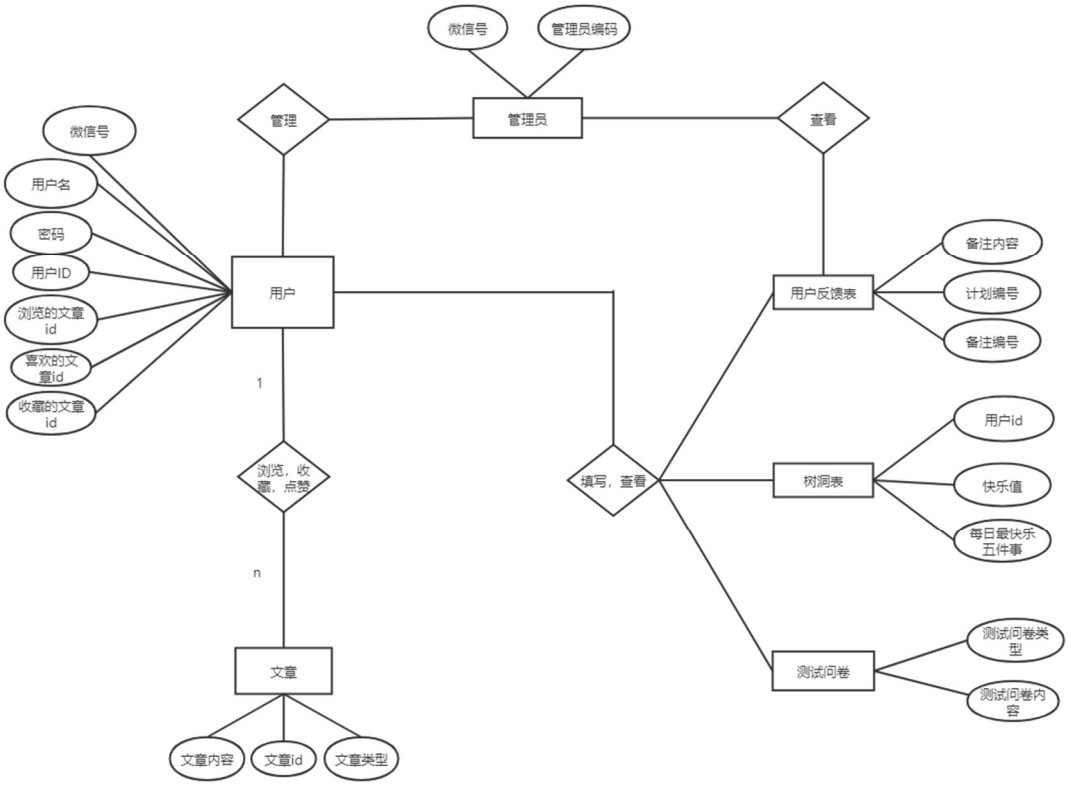
2.系统总体设计

2.1 软硬件运行环境约束

本系统程序基于 JSP 开发，使用 Sqlserver 数据库。开发平台: Win10。
总之本系统对运行软件的要求不高，主要支持 Chrome 浏览器。
系统所需要的硬件配置: 运行在 64 位或 32 位操作系统。
软件:操作系统: Win10
支持环境: Microsoft IIS。
浏览器: Chrome 等.。
数据库: SQL Server 2019。
编程语言:java，Javascript，html。
设计工具: Microsoft Visual studio 2017。

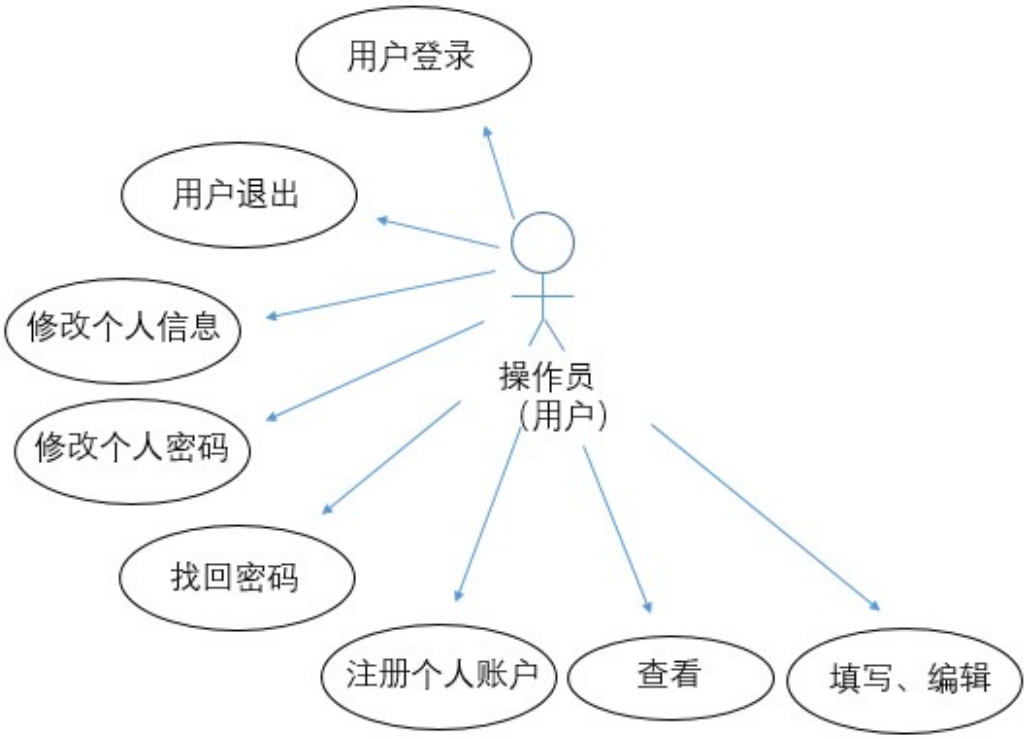
2.2 系统体系结构

ER 图

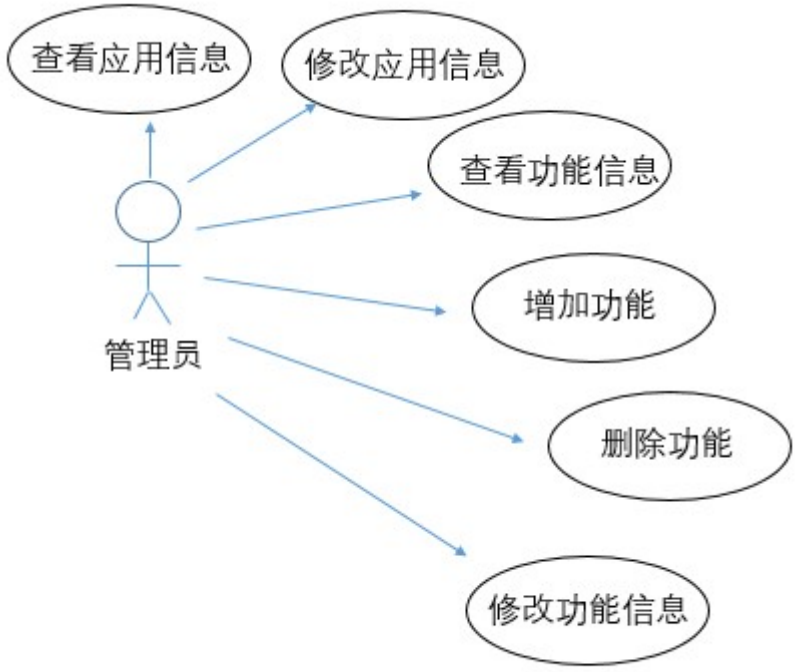


2.3 权限设计

2.3.1 用户用例图



2.3.2 管理员用例图



3.程序接口设计

功能编号	功能名称	功能简述
A1	用户模块	用户查看管理自己的各类信息。
A2	管理员模块	管理用户上传信息以及数据库管理。

功能编号	子功能编号	子功能名称	子功能简述
A1	A1-1	注册	用户通过手机号注册成为正式用户
	A1-2	登录	使用现有微信号登录小程序
	A1-3	浏览文章	① 查看发布在小程序的文章
			② 收藏点赞功能
	A1-4	测试问卷	①测试收集功能
			②生成测试结果

	A1-6	树洞记录	①编辑保存日记功能
			②查看已保存日记
A2	A2-1	用户管理	①查看收集用户反馈表
			②处理用户登录注册信息
	A2-2	更新数据库	①查看收集用户反馈表
			②每日更新文章，推送
			③更新测试问卷

4.数据库设计

见《数据库设计说明书》

5.安全性设计

5.1 隐患

设计缺陷导致的意外行为：数据丢失、软件出现 bug、用户数据泄露
用户行为：恶意输入、用户越权访问或操作、恶意盗号

5.2 解决

5.2.1 用户行为

1.尽可能实现用户的权限最小化

应用用户的权限最小化，控制应用用户对文件、数据的访问，记录并统计登录历史；对重要信息资源设置敏感标记并控制对设置敏感标记资源的操作。

2 .对前端输入信息进行验证

将输入验证策略作为应用程序设计的核心要素。假定所有的输入都是恶意的，不要依赖于客户端的验证，虽然使用客户端验证可以减少客户端和服务器之间的信息传递次数。

要做到限制、拒绝或者净化输入，输入验证的首选方法是从开始就限制允许输入的内容。按照已知的有效类型、模式和范围验证数据要比通过查找已知有害字符的数据验证方法容易。设计应用程序时，应了解应用程序需要输入什么内容。与潜在的恶意输入相比，有效数据的范围通常是更为有限的集合。为了使防御更为彻底，可能还需要拒绝已知的有害输入，达到净化输入的效果。

3. 对密码加密

应用系统应对系统的使用用户密码进行加密（可以是软加密），包括密码的产生、密码录入、密码修改、密码的传输、密码的保存。软加密时应确保软加密算法具有足够的强度，并且确保密钥存储安全，对密钥的访问应严格控制。同时，还应采取必要的措施，确保软加密算法的安全。

4. 提供应用系统用户的身份识别功能

身份识别是信息安全服务的基础，基本原则是要做到用户区分的唯一性，认证是基于身份识别的，身份识别最常见的形式就是用户 ID，与密码组合标识一个用户身份。

5.界面的设让用户明确自己的权限，明确自己能够进行的操作，不让用户误以为拥有实际上没有的权限。

6. 限制第三方对加密文件的操作权限啊，比如只允许浏览，禁止复制、剪切、截屏、修改

等操作，设置好查看次数和截止打开日期等。

5.2.2 设计行为

设计行为：

1.降低软件和接口的复杂性

接口和软件的复杂容易导致程序出现不可预料的错误,简化接口能有效避免这种错误出现的机率。

——单元的代码长度控制在 66 行到 132 行

——模块有唯一的入口和出口

——模块循环有正常退出条件

——清晰定义模块的所有输入输出并进行范围检测

——设计文档明确标识出所有安全性关键的设计要素

2.提高软件的健壮性

——接受错误输入，输出错误提示信息，软件能判断出操作员的输入操作正确性，在遇到不正确(或不合理)输入和操作时，软件拒绝该操作的执软件提醒操作员注意错误的输入或操作 软件指出错误的类型和纠正措施

——对输入参数进行合法性检查，对非法参数进行处理，返回错误代码

2.算法与数据管理

——对于规定时间内完成规定时间的模块应使用规定时间内得出结果的算法

——用统一的符号来表示参数、常量和标志，以便在不改变源程序逻辑的情况下,对它们进行修改

——文件必须唯一且用于单一目的；文件在使用前必须成功地打开,在使用结束必须成功地关闭；文件的属性应与对它的使用相一致。

——对关键下标，在使用前进行范围检查

——慎用易错架构：浮点数，指针，递归，中断，继承，别名，无界数组，动态内存分配，全局变量，公共数据和公共变量

3.风险隔离

——划分模块,防止组件之间特殊的相互作用和交叉耦合干扰;减少软件验证过程的工作量;最小化安全相关组件的规模

——运用信息隐蔽技术，使信息仅对有权和需要访问它的程序开放。信息隐蔽可以避错的三个理由：降低了信息意外讹误的概率；可以帮助在程序中建立防火墙,降低信息问题影响的范围；由于信息被局部化,程序员更少地产生错误,验证人员更容易找到缺陷。

常见需要隔离的信息：

安全关键的数据

容易被改动的区域

复杂的数据

复杂的逻辑

在编程语言层次上的操作

4.异常处理

内部异常处理

1）在运行阶段，对于预期范围内的异常，异常处理措施应保证系统处于安全状态，并持续运行

2）在运行阶段，对于超出预期的异常，异常处理措施最低限度应使系统转入安全状态
3）在异常发生之后，采取措施，保证数据的完整性
4）在异常发生之后，采取措施，保证敏感和关键数据不被泄露
外部异常处理
1）周期性检测外部输入/输出设备的状态，并在发生失效时转到到某个安全状态
2）对于非法的外部中断，软件应能自动切换到安全状态