西华大学计算机与软件工程学院毕业设计（论文）开题报告

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 专业 | 信息安全 | | | |
| 题目 | 跑腿服务系统的安全设计与实现—系统安全设计与实现 | | | |
| 学生 | 龙代权 | 学号 | | 3120190906226 |
| 指导  教师 | 杨毅 | 工号 | | 0119970049 |
| 选题的背景、意义、及相关研究（技术）现状 | 1. 选题的背景、意义、及相关研究（技术）现状    1. 选题的背景   近年来,随着移动互联网的发展,各种基于移动端的生活服务平台应用层出不穷。跑腿服务作为一种新兴的生活服务方式,借助移动端APP,通过调度一定数量的跑腿人员,为用户提供生活中各种送货、代取等服务。由于涉及到用户个人信息、资产等,跑腿服务系统面临一定的安全风险,如用户信息泄露、跑腿人员身份认证缺陷导致的欺诈行为等。因此,在跑腿服务系统的设计与实现中,安全机制的考虑显得尤为重要。该课题拟研究跑腿服务系统可能面临的安全风险,并提出相应的安全设计与实现方案,以确保系统和用户资产的安全。  1.2 选题的意义  在21世纪的今天，我们在享受科技带来便利的同时，也无时无刻不在面临着个人隐私泄露的风险。随着移动互联网技术的发展和普及，跑腿服务系统已经成为了现代生活中不可或缺的一部分。然而，随之而来的安全挑战也越来越多。构建安全、可靠的跑腿服务系统对于用户的个人信息和财产安全具有至关重要的意义。因此，研究跑腿服务系统的安全设计与实现，对于提升系统的安全性，保障用户利益具有重要意义。同时，本文的研究成果也有望对未来的个人发展奠定一份安全基础。因此，该课题的研究具有重要的理论和实践意义，值得进一步深入探究。  1.3 创新性、先进性、实用性  (1) 创新性：近年来各大公司对Flutter技能的要求越来越高，甚至设立了专门岗位，但掌握Flutter高阶技能的人才寥寥无几，Flutter高阶人才缺口大，西华大学并未开设Flutter课程，学生需要自主学习，采用Flutter 技术进行系统开发，发挥Flutter技术的专长和良好特性。另一方面，跑腿服务系统的安全问题是当前互联网应用领域的热点问题之一，本项目致力于研究针对该问题的解决方案。因此不管是从开发技术的储备还是从安全问题的研究均具备一定的创新性。 (2)先进性：本项目采用Flutter技术，与以往的技术相比。Flutter具有以下几个特点：①跨平台：Flutter支持多平台如Mac OS、Windows、Linux、Android、iOS，良好的跨平台性，大大减少了开发成本。②体验顺滑：使用内置的Material Design（android风格）和Cupertino（ios风格）风格组件，以及丰富的motion API,平滑而自然的滑动效果和平台感知，为用户带来全新的体验③响应式框架：使用一系列基础组件和响应式框架，可以轻松构建用户界面。使用功能强大且灵活的API可以实现复杂的界面效果。④支持插件：使用插件可以访问平台本地API,如相机，蓝牙，WIFI等等。借助现有的Java，swift ,object c，c++代码实现对原生系统的调用。同时，本项目将结合当前最新的技术手段和安全策略，采用系统化的研究方法，对跑腿服务系统的安全设计和实现进行全面的深入研究。 (3)实用性：现今，跑腿服务已经成为人们生活所不可或缺的一项服务，受众广，人口基数大，就难以避免的会出现各种数据泄露的风险。就比如国内大厂：京东、淘宝、美团等，都出现过各种安全问题。本项目研究成果将为跑腿服务系统的设计与实现提供实用的技术支持和指导，降低系统被攻击或出现安全漏洞的风险，提高用户的使用信任度，具有重要的实用性。  1.4 相关技术现状  本项目采用自上而下逐步开发，前后端分离，角色和功能分开设计，团队成员协同开发。这样使软件开发流程更加有条理、功能设计更加自由化，方便后期对不同功能进行更改。  本项目主要划分为六大流程，分别是数据库设计、系统框架设计、UI设计、用户角色设计、核心功能设计、安全方案设计。因为是团队项目，我们将整个流程划分后进行协同开发。本文主要研究的是系统框架设计、核心功能设计和安全方案设计。开发的主要内容包括，完成整个系统的流程分析和设计、技术储备分析、功能模块划分，与团对实现核心功能开发，其中安全设计需要贯穿整个开发流程，包括但不限于数据库安全，网络数据安全等。 本项目采用跨平台移动应用开发框架Flutter以及同时支持JIT与AOT的Dart语言。具有运行速度快、执行性能好、开发效率高等特点。本项目的开发工具使用的是Android Studio 并且由于是移动应用，所以可以使用Android Studio自带的AVD Manager 来创建手机模拟器。由于本项目是团队项目，需要及时沟通进度及进行代码的整合。因此使用基于Git的代码托管服务Github，将代码及时更新上传到仓库，方便整合。  本项目拟采用的关键开发技术或框架包括：Flutter, Dart  (1) Flutter  Flutter[1]018年Google发布的跨平台移动UI框架，是一款移动应用程序SDK，一份代码可以同时生成iOS和Android两个高性能、高保真的应用程序。具有以下特征：第一，跨平台应用的框架，没有使用WebView或者系统平台自带的控件，使用自身的高性能渲染引擎自绘。第二，简化版的浏览器最大限度在Android和Ios上统一UI，包括业务逻辑和用户体验。第三，开发语言使用Dart，结合C, C++, 和Skia构建，支持hot reload包含着完整的控件和工具链。Flutter可以通过Dart编译定义，无需JSX或者XML那样的声明式布局语言，容易阅读和可视化，并且在开发过程中无需搭建可视化界面，因为hot reload可以让我们在手机上立即看到效果。第四，控件是每个Flutter应用程序的基本构建块，和分离视图、布局、控制器以及其他属性的框架不同，Flutter具有一致的统一对象模型：控件。一个控件可以定义：结构元素（比如按钮或菜单）、风格元素（比如字体或颜色方案）、布局的方面（比如填充）以及一些业务逻辑。第五，组合大于继承，控件本身往往由多个较小型的、单一功能的控件所构成，结合在一起形成强大的效果，类的层次结构往往是扁平的，以最大化可能的组合数量。  (2) Dart  Dart[2]的语法和C语言十分的类似，是一种面向对象的、类定义的、单继承的语言。在Dart中，一切皆为对象，所有的对象都从Object类继承而来。Dart支持各种编程辅助工具，也支持泛型、顶级函数、顶级变量等，是一种强类型语言。最初Dart的开发是想要取代JavaScript，吸取了Java、C这些热门语言的优点，但是效果不尽如人意。直到Flutter的出现，同为Google旗下的开发团队Dart以及Flutter的绑定使得这对组合快速发展起来。到Dart 2时，更是发布了许多为Flutter量身定制的功能。并且Flutter及Dart的生态有Google的支持，在发布了Dart VM后，Dart可以更快速的进行开发而不必编译为JavaScript。而且Dart使用Isolate模式，每个Isolate都拥有自己的私有堆，所以他的垃圾回收不会对其他的进程造成影响也就避免了卡顿等现象的出现。总的来说，Dart与Flutter的相互配合让未来前景一片良好。 | | | |
| 研究（设计）的主要内容和预期目标 | 1. 设计的主要内容和预期目标   2.1 设计的主要内容  2.1.1团队任务  区别于市面上跑腿类APP，内容花里胡哨，广告多，需要迎合更多人需求，我们致力于开发一个内容简介，方便使用， 只针对某大型住宅需求的APP。  团队任务包括如下细节：  （1） 数据库需求分析和设计：完成本系统数据建模、数据库需求分析、数据库物理设计、视图、触发器和存储过程等。  （2） 系统框架设计：完成整个系统的流程分析和设计、技术储备分析、功能模块划分。  （3） UI设计：使用当前社会主流UI技术实现界面和风格统一，使用流行框架实现，界面友好。界面元素有创意，设计风格体现简洁与美观的统一、技术与艺术的结合，且与开发内容的风格相符；操作流程合理、不繁琐。  （4） 用户角色设计：根据实际应用，必须严谨分配各角色功能，且超级管理器可以动态配置各角色功能。  （5） 主要功能及管理：以实际应用为准，实现对跑腿服务系统中各个环节的管理（用户管理、订单类别管理、下单功能、抢单功能、订单流程管理、地图和路线规划、支付（可虚拟）、意见和投诉管理、互动交流等。  （6） 网络数据安全：防止非法SQL注入访问数据、防DDos攻击、其它web入侵防御、恶意订单控制。  （7） 数据管理：包括数据提交，基本的增、删、查、改；管理员的数据维护功能。  （8） 数据库安全设计：数据库用户角色标识和鉴别、存取访问控制、关键数据加密存储、事务管理等。  （9） 编程：代码实现以上所有功能，并在合适的数据量情况下测试和分析，并给出测试报告。  2.1.2个人任务  个人任务包括：  （1） （团队任务 2. 系统框架设计）  （2） （团队任务 5. 主要功能及管理后台部分设计和编码  （3） （团队任务 6. 网络数据安全）  （4） （团队任务 7. 数据管理，协助其它同学完成后台部分数据管理）  （5） （团队任务 8. 数据库安全设计）  （6） （团队任务 9. 编程和测试）  2.1.3 系统（或算法）架构图（组成图）及说明    图2-1 系统组成图  本跑腿系统根据不通用户由不通功能组成。  针对普通用户，主要由订单和用户两个模块组成。在订单模块中，用户登录系统以后可以在此下订单发布需求，系统将根据用户所选的地点计算出所需金额，然后吊起内置支付方式进行支付，支付完成后用户可以查看该订单相关信息，包括下单时间，支付金额，跑腿人员联系方式等。在用户模块中，用户可以修改用户名，密码等基本信息，还能对平台做出投诉和建议，同时我们还添加了一个客服按钮，点击后将跳转到客服聊天窗口，有任何问题都可以向客服进行反馈。  针对跑腿用户，在登陆后可在订单界面对普通用户发布的需求进行抢单操作，完成订单后平台会将收益发放至跑腿用户账户，用户可对该订单具体信息进行查看。用户模块除了没有投诉之外，其它和普通用户界面基本相同。  针对管理员，可对所有用户进行管理，包括拉黑、重置密码等，还可对所有订单进行相关操作，包括删除订单，修改金额等，也可对普通用户的意见进行管理，包括删除无视意见，回复意见等。  2.2 预期目标  作为团队项目，本人负责系统框架设计、核心功能实现以及安全方案设计，主要的预期目标是通过毕设课题的经济效益与社会贡献分析；通过毕设课题与法律、法规、健康、安全、环境等因素的关联分析；通过技术选型对比分析或算法差异对比分析。主要实现软件《跑腿服务系统》如下功能模块的开发、调优以及测试。   1. 订单管理功能，包括下单、抢单的具体实现 2. 支付功能模块，添加市面主流支付功能，如微信、支付宝 3. 客服模块，完成内置聊天窗口的添加 4. 路线规划功能，调用市面上成熟的地图API实现路线规划和自动计费 5. 系统安全测试，对各种常见安全威胁进行测试，尽量做到将安全风险降到最低 | | | |
| 拟采用的研究（设计实现）方法、步骤 | 1. 研究（设计实现）方法、步骤   3.1 系统（或算法）流程图及说明    图3-1 系统流程图  在登陆界面，拥有账号可以直接登录，需要输入账号和密码，登录会跳转到验证界面，输入短信验证码即可成功登录。通过验证码技术保证用户真实性，以及提高账户安全性。若没用账号可以先进行注册再登录。登录失败会弹出消息框提示，当失败次数达到五次后将锁定账户。验证成功后进入系统界面，在导航栏有首页、订单和我的三个模块。用户可以在首页可以查看大致位置信息，可以通过该界面下单，跑腿用户会在该界面展示出附近的订单信息，可根据实际情况抢单。在订单模块普通用户和跑腿人员可以看到自己的当前或过去的订单信息，点击订单还能查看更详细的信息。在个我的界面可以进行用户基本信息的修改，以及联系客服，普通用户还能进行投诉或建议。  3.2关键技术/算法步骤  在本系统中最核心的技术就是抢单算法的设计与实现和网络数据安全的实现。  抢单过程是一个互联网高并发场景，因此实现系统的抢单功能需要解决多人同时抢单的高并发问题。还需要对这以范围内的跑腿用户进行筛选，选择合适距离范围内的跑腿人员可以进行抢单。抢单功能通过多线程的方式进行实现，根据下单人填写的始末位置和闲置的跑腿人员的位置计算出最优距离并且按距离降序排序，向适合距离范围内的跑腿人员发布抢单信息。最优距离的算法是根据跑单信息的始末位置和跑腿人员所在位置综合计算出的最短路径，在某路径范围内的跑腿人员才能收到抢单信息。  随着各种应用越来越广泛,当程序受到攻击时会造成严重的数据泄露和财产损失,因此解决网络数据安全问题十分重要。终端应用程序面临的主要安全威胁包括Android Manifest[3]配置相关的风险或漏洞，主要表现为XML配置文件相关功能被打开，造成APP可被调用或数据可被打开；WebView组件及与服务器通信相关的风险或漏洞、数据安全风险等。  为了预防这些攻击，需要在开发完成后关闭所有可调试功能，仔细配置Android Manifest，减少内部组件暴露的风险，同时对应用文件权限的调用做严格限制，还需要对敏感数据做安全加密，包括但不限于用户账号、密码、个人信息等重要数据。  针对数据库安全设计包括以下方案：  （1）SQL注入攻击：使用参数化查询，即将用户输入的数据以参数的形式传递给SQL查询语句，而不是将用户输入的数据直接拼接到查询语句中。使用参数化查询可以防止SQL注入攻击，同时也可以提高程序的性能和可读性。  （2）不安全的密码存储：如果密码明文存储在数据库中，那么一旦数据库被攻破，所有用户的密码都会被暴露。解决方案是使用加密算法对密码进行加密存储。常用的加密算法包括MD5、SHA-256、bcrypt等，这里使用MD5加密。  （3）数据库权限控制不当：如果数据库权限控制不当，黑客可以通过一些手段获取管理员权限，从而对数据库进行恶意操作。解决方案是设置强密码，并且为每个用户分配不同的权限。管理员应该只授予必要的权限，其他用户只能访问他们需要的数据和功能。  （4）数据库备份和恢复不当：如果数据库备份和恢复不当，数据可能会被恶意篡改或丢失。解决方案是定期备份数据库，并将备份存储在安全的地方，同时测试数据库恢复过程以确保备份的可靠性和完整性。  （5）数据库连接信息泄露[4]：如果数据库连接信息泄露，黑客可以利用这些信息对数据库进行攻击。解决方案是将数据库连接信息存储在安全的地方，例如服务器配置文件或者环境变量中，并且限制只有授权的用户才能访问这些信息。  3.3 UI设计  3.3.1 设计理念  在UI设计[5]中,我们要遵循简洁、直观的原则,让用户在使用APP时能够快速理解界面,轻松完成操作。具体来说:  （1）界面元素应简单明了,不要有过多的装饰;  （2）版面布局要合理,内容区、功能区、导航区等要区分开来,不要过于拥挤;  （3）图标要符合用户的习惯,让用户一眼就能看懂;  （4）文字描述要简短明了;  （5）页面跳转要合理,让用户不会感到困惑。  这些UI设计理念,可以让我们的APP更易于使用和理解,提高用户体验。  3.3.2 拟设计的布局与操作  首先是登录界面，当用户是第一次使用时需要先进行账户的注册。为了账户的安全，在登陆时将会进行账号密码的验证，一旦验证失败次数大于五次就会将账户锁定。此时需要用户进行认定才能解除锁定。    图3-1 登录与注册界面图  在验证成功进入系统后，会停留在首页。下边导航栏固定，上面部分会通过地图大致显示用户位置信息，中间的菜单栏用户可根据需求选择取送物品，dianji1填写取收件信息可填写详细信息，便于跑腿用户接单，填写成功后点击下单付款即可。    图3-2 普通用户首页界面图  通过底部的导航栏可以跳转到其他的模块，如下图，在订单界面图上。用户可以查看正在进行的订单和已经完成的订单，点击订单还能看到更详细的信息，顶部的搜索栏还可以对订单进行搜索。方便用户对订单进行管理    图3-3 订单界面图  在我的界面，用户可对自身信息进行管理等。    图3-4 骑手我的界面图   1. 参考文献：   [1] Flutter中国开源项目. Flutter实战·第二版[OL]. <https://book.flutterchina.club>  [2]百度百科[OL]. https://baike.baidu.com/item/DART/22500518  [3]知乎. Android 应用有哪些常见，常被利用的安全漏洞?[OL]. <https://zhuanlan.zhihu.com/p/352583797>  [4]CSDN. 数据库连接泄露的问题[OL]. https://blog.csdn.net/u012089657/article/details/48897151  [5]李时颖,马俊伟.基于用户体验的UI设计要点分析[J].电脑知识与技术,2017,13(36):70-72. | | | |
| 进度安排 | 起讫时间 | | 计划完成内容  (一般可分为资料文献收集、拟定方案提纲、试验或概要设计、详细设计或初稿、定稿等阶段) | |
| 2022年 10月7日-2022年10月15日 | | 料文献收集，课题调研，技术路线，可行性分析 | |
| 2022年10月16日-2022年10月31 日 | | 系统整体方案（概要）设计 | |
| 2022年11月1日-2022年11月24日 | | 功能模块（详细）设计 | |
| 2022年11月25日-2023年4月15日 | | 编写功能代码 | |
| 2023年4月16日- 2023年5月30日 | | 撰写设计说明书等文档，完成翻译，准备答辩 | |
| 签名 | 学生签名： 年 月 日 | | | |
| 指导教师意见 | 指导教师签名： 年 月 日 | | | |
| 系部（开题小组）意见 | 签名（系主任或开题小组组长）： 年 月 日 | | | |

版本：2021.12

注：不足部分可加页。