# 摘要

本论文探索了一种新手机APP哲学：无需安装注册，根据环境主动推送，即点即用。

本论文实现了可以支持这样一种新APP范式的框架和网络结构，挖掘了这种新范式可带来的便利性与机会，探索了这种范式技术上的挑战，并针对性地提出了创新的解决方法。

关键字：小程序，LBS，前端构建，前端动态链接，分布式内容分发，数字签名鉴权与支付，HTML5，Hybrid App

# Abstract

# 目录

[引言 1](#_Toc514699772)

[国内外相关研究状况综述 1](#_Toc514699773)

[微信扫码打开小程序 1](#_Toc514699774)

[设计目标、与现有方案的区别 2](#_Toc514699775)

[目标与哲学的概述 2](#_Toc514699776)

[和微信扫码打开小程序的不同 2](#_Toc514699777)

[使用上的不同 2](#_Toc514699778)

[哲学、目的、定位上的不同 3](#_Toc514699779)

[应用运行容器 4](#_Toc514699780)

[基于WebView的容器 4](#_Toc514699781)

[基于JavaScript引擎，但使用原生View的容器 4](#_Toc514699782)

[直接运行原生代码 4](#_Toc514699783)

[本论文的选择 5](#_Toc514699784)

[应用分发与压缩技术 6](#_Toc514699785)

[编译时拆分依赖库和代码主体 6](#_Toc514699786)

[动机 6](#_Toc514699787)

[实现方法分析 6](#_Toc514699788)

[实现 6](#_Toc514699789)

[根据哈希值存储依赖库或业务代码 7](#_Toc514699790)

[运行时动态拼装与链接APP 7](#_Toc514699791)

[在NAT内部部署CDN节点 7](#_Toc514699792)

[其他可以探索的技术 8](#_Toc514699793)

[brotli压缩 8](#_Toc514699794)

[预先压缩 8](#_Toc514699795)

[网络总架构设计 9](#_Toc514699796)

[总架构图 9](#_Toc514699797)

[主数据管理服务器 9](#_Toc514699798)

[应用仓库服务器 10](#_Toc514699799)

[镜像自动同步 10](#_Toc514699800)

[通过DNS解析进行就近分发 11](#_Toc514699801)

[Docker容器 11](#_Toc514699802)

[应用分发效果分析 13](#_Toc514699803)

[字节传输量（使用拆分技术与不使用拆分技术） 13](#_Toc514699804)

[传输耗时 13](#_Toc514699805)

[移动数据流量消耗 13](#_Toc514699806)

[基于数字签名的用户鉴权支付 14](#_Toc514699807)

[总设计思路 14](#_Toc514699808)

[用户鉴权流程 14](#_Toc514699809)

[前端流程 14](#_Toc514699810)

[后端流程 14](#_Toc514699811)

[用户支付流程 15](#_Toc514699812)

[支付时序图 15](#_Toc514699813)

[用户信息请求 16](#_Toc514699814)

[基于地理位置的服务发现 17](#_Toc514699815)

[WIFI网络内的服务发现 18](#_Toc514699816)

[实现原理 18](#_Toc514699817)

[路由器DNS解析的配置 18](#_Toc514699818)

[可能问题与解决方案 19](#_Toc514699819)

[其他可能方案 19](#_Toc514699820)

[端口扫描 19](#_Toc514699821)

[广播 19](#_Toc514699822)

[默认网关上配置专属程序 19](#_Toc514699823)

[安卓客户端的实现 21](#_Toc514699824)

[Cordova代码的改造、运行多个APP 21](#_Toc514699825)

[用户数据的管理 21](#_Toc514699826)

[APP发现的实现 22](#_Toc514699827)

[本地APP代码缓存 22](#_Toc514699828)

[鉴权和支付的能力 23](#_Toc514699829)

[桌面小工具 23](#_Toc514699830)

[拓展JavaScript能力 24](#_Toc514699831)

[基于开源项目cordova 24](#_Toc514699832)

[管理公钥私钥和签名 24](#_Toc514699833)

[JavaScript中调用原生接口 24](#_Toc514699834)

[安全地弹出用户许可框 24](#_Toc514699835)

[PC运行环境的兼容处理 25](#_Toc514699836)

[应用场景探索 26](#_Toc514699837)

[停车场缴费 26](#_Toc514699838)

[餐厅点菜 28](#_Toc514699839)

[在线考试 29](#_Toc514699840)

[会议时刻表 31](#_Toc514699841)

[活动报名 32](#_Toc514699842)

[应用场景的总结、畅想与商业可能 33](#_Toc514699843)

[完全去中心化可能性的探讨 34](#_Toc514699844)

[附录：PoC版本代码链接 36](#_Toc514699845)

[design 36](#_Toc514699846)

[demo-apps 36](#_Toc514699847)

[app-builder 36](#_Toc514699848)

[app-repo-server 36](#_Toc514699849)

[android-app 36](#_Toc514699850)

[app-auth-demo 36](#_Toc514699851)

[central-server 36](#_Toc514699852)

[mirror-tool 36](#_Toc514699853)

[总结 37](#_Toc514699854)

[致谢 38](#_Toc514699855)

[参考文献 39](#_Toc514699856)

# 引言

手机APP在人的日常生活中扮演越来越重要的角色，APP数量更呈爆炸性增长。每个人的手机里都有好几屏的APP，但真正经常使用的APP却并没有几个。

很多APP用一两次就丢弃，或只会在某个特定场合、地点使用的。这些APP耗费了用户精力下载、注册，但实际使用频率很低，还占用了手机屏幕上的一个格子。

我的思考是：对于办公类APP或微信等APP，我们的确应该安装。但对于地点相关APP（如博物馆导览、商场导览、停车缴费、餐厅等位/点菜），安装并不是最好的选择。

用户极有可能会因为不知情、嫌麻烦等原因不安装APP，这样服务就无法抵达用户，商家辛苦开发的APP产生不了任何价值。就算用户安装了，这件事情对用户来说也是不好的，因为很快他的手机屏幕上就会布满他不会再想使用的APP。

更好的一种范式，或许是把手机视为一个与周围环境产生交互的接口，把手机APP作为用户个人能力和意愿的拓展。比如：回到家后手机屏幕上自动显示智能家电APP让用户调空调开电视；坐到车里手机屏幕上自动显示车况与导航信息；进了饭店手机屏幕上自动显示菜单与在线点菜；在地下车库时手机屏幕自动显示寻车导航和在线缴费的APP。

本论文就实现了这样一种新型APP范式：一个支撑它的网络、一系列开发者标准和工具、一个能运行它的安卓客户端。

要做到最好的用户体验，不仅需要能根据地理位置和环境主动为用户发现APP，更要让用户能够一键瞬间打开APP、免去用户注册不同APP的麻烦。

APP分发策略是一个需要重点研究的话题，如何保证APP的迅速下载、即点即开，如何避免用户产生高昂的流量费用。本论文用一种综合而又创新的方案试图解决本问题。

最后，本论文挖掘了这种新型APP范式的使用情景、对5种使用情景做了样例APP、并探索了潜在的商业价值。

## 国内外相关研究状况综述

### 微信扫码打开小程序

国内和本论文做的事情最接近的是微信通过扫码打开小程序，微信的方式已经在各大商业广场被广泛使用，取得了不错的成果。本毕业设计和微信扫码小程序的对比请看“和微信扫二维码打开小程序的不同”一节。

# 设计目标、与现有方案的区别

## 目标与哲学的概述

设计的目标可以概括为：让手机成为和周围环境交互的入口、APP无需再安装，即点即用。想达到的效果是：用户走到任何地方，手机上都自动跳出和该位置有关的手机App，并以最小的数据传输量自动下载到本地，用户点开就可以使用。

关键字在于“主动推送”，“一键”打开APP。因为哪怕多一个步骤都会让很大比例的用户放弃使用，只有把方便做到极致，用户才能体验到用手机操办周围环境中一切的快感。

关键字还在于，和环境相关——APP只在用户身处某个环境时显示，在用户离开那个环境后就隐藏。这样，手机上就只显示会被用到的APP，还用户一份清静。

设计的哲学是：让手机真正成为一个与周围环境发生交互的平台，成为用户能力的延伸。

## 和微信扫码打开小程序的不同

### 使用上的不同

本毕业设计旨在把整个APP启动过程加速到最快，使用体验上还是会和微信有很大的区别。

拿停车场缴费为例，要在微信上实现停车场缴费，你需要：

1. 点开微信

2. 打开扫一扫

3. 对准二维码，对焦，调整到扫出来为止（光线差的环境下，扫二维码并不快）

4. 关注微信公众号

5. 在微信公众号菜单中找到停车场缴费功能

6. 等待微信的加载条从0加载到100（取决于网络环境，通常要好几秒）

7. 输入自己的车牌号

8. 缴费

而使用本论文中的方案，你只需要：

1. 点开早已在手机主屏等候的停车场App

2. 如果是第一次运行类似程序，则输入自己的车牌号（否则可以直接通过用户信息授权的方式自动输入）

3. 缴费

原方法相比较而言，过程繁琐、耗时长。在这种情境下，缴费的方便程度对顾客是否会选择这样的缴费方式有至关重要的影响。如果二维码对焦不上扫不出、网速慢，他们都会选择放弃。

换成新方法后，便利程度还是能提高不少的，主动推送的特性能让比较懒或搞不清如何扫码的用户更有可能使用商家开发的服务性APP。

### 哲学、目的、定位上的不同

哲学和目标定位上，本论文也和微信有着很大的不同。

哲学上，微信的哲学是连接、关注，更注重的是把每一位客户和商户连接在一起。所以微信做公众号和基于公众号上的小程序。而本论文注重的是服务、体验，只在意用户是否可以在最短的时间内实现他的意愿。

目标和定位上，微信的目标是把商户作为整个庞大微信生态圈的一环，让商户依赖微信、互利共赢，在给商户提供便利的同时巩固微信在使用者那边的地位。而本毕业设计做的是一种开放式的标准，就像一种协议一样，给所有人带来便利却不被某一个机构所掌控。

# 应用运行容器

手机操作系统本身是一个应用运行的容器，本论文计划做出的产品是一个手机操作系统之上的应用运行容器（一种虚拟容器）。它的本质是另一个手机APP，但手机APP也可以充当应用运行容器的角色，让一个手机APP动态运行别的虚拟APP，大致有以下三种方法：

## 基于WebView的容器

这种方法使用最为广泛，是“hybrid app”最早的含义，代表解决方案有cordova、PhoneGap。

它的本质就是把网页包在一个原生APP的容器里（原生APP只有一个内嵌的网页，显示被嵌入的HTML5网页），达到HTML5 APP看起来是一个原生APP的效果。

除此之外，这种方案还能解决一个额外的问题：WebView的局限性。WebView是不能读本地文件的、也没有接口让WebView打开闪光灯等，但这种方式做的APP可以在WebApp和原生容器之间通过类似ipc的技术建立起一个通道。WebView把调用原生接口的意愿告诉原生容器，原生容器进行调用并把结果通过ipc返回给WebView。这样就相当于WebView有了调用任何原生接口的能力，在能力上能做到和原生APP等同。

这种方案有很多优点：跨平台（一次开发，各种手机操作系统使用）、开发便捷（使用HTML5的技术）、健壮稳定（是历史最悠久的混合APP开发技术）。

缺点主要在于：性能较低，WebView中运行的是HTML、CSS，和渲染原生组件相比，WebView执行渲染时复杂很多。因此尤其在低端机型上，会略微卡顿、无法达到60fps。

## 基于JavaScript引擎，但使用原生View的容器

这种方法近几年来比较流行，代表解决方案有react native和native script。阿里巴巴的Weex和腾讯的微信小程序也均是使用这种方案。

它同样使用JavaScript运行时作为代码的执行器，不同的是，它不再使用WebView来做界面的呈现，而是使用ipc的方法， 让JavaScript动态地告诉原生宿主APP，要渲染什么原生组件、放在什么位置。

好处是解决了WebView的性能问题，因为真正使用原生组件，所以真正有原生APP的流畅体验和交互风格，也能到达60fps。

坏处是这种方案和WebView比稳定性不那么好（因为是新方案、和native打交道更多），可定制性没那么强（界面是原生组件+属性，和webview强大的css比起来弱一些），有些效果难以找到跨平台一致的原生组件，必须为不同的操作系统写不同的代码。

## 直接运行原生代码

以上两种方法都是使用到JavaScript来支持自定义程序的，因为基于JavaScript引擎的方案不涉及到原生代码的编译，比较稳定可行。直接运行原生代码的方案也有，如直接动态下载和修改安卓的.dex，腾讯的tinker可以做这样的热修复。

但直接运行一个崭新APP的原生代码，这种方案应当还不存在。这样的话相当于一个APP替代了操作系统一部分的功能，需要有所有的APP权限。很有可能操作系统会在APP权限、资源分离、元数据定义等方面给这种方案设置阻碍。

## 本论文的选择

本论文还是选择最成熟、使用广泛的技术，来作为应用运行容器的基石。

本论文选用Cordova作为基础，在修改Cordova的代码之上添加各种新特性，来实现所有的功能。

# 应用分发与压缩技术

要做到瞬间打开APP、主动推送，APP的传输是一个要仔细考虑的技术难点。

要开辟一个新的专用信道来做这件事情，并部署到全世界，是不可能的，所以还是要使用因特网（TCP/IP）。如果只是简单地下载APP，因为每个APP动辄几十兆，所以用户的流量很快就跑光了，这样性价比太低了。

如何做到主动推送、秒开、节省流量，这是本毕业设计最大的难点。

## 编译时拆分依赖库和代码主体

### 动机

一个HTML5 App中，除去图片，剩下的体积基本都是JS代码。

负责业务逻辑的代码和依赖库代码比起来少之又少。拿停车缴费程序为例，程序员自己可能只写3000行代码，但它依赖的ionic有10000行代码、Angular框架有30000行代码、lodash有20000行代码、Bootstrap有2000行代码。

因此，本论文创新地想到了分拆的方法，把APP的业务代码和依赖库代码分开，所有依赖库代码只传输一遍，之后，只传输业务代码而不传输依赖库代码。这种分拆、运行时动态组装的方式可以大大减少传输体积。

### 实现方法分析

JS的包管理系统已经相当完善，比较现代的JS前端都会使用npm包管理（类似maven）。

npm中，一个项目会有一个package.json，其中会定义它的所有dependency（也是npm包），和它的主入口（index.js）。

因此，HTML5 App在发布时，可以参考package.json进行分拆操作，即抽取所有dependency的代码分开打包，留下index.js的代码和dependency说明的元数据。

打包成这种格式之后，在运行时，容器只需要下载用户代码包和本地缺少的dependency，将它们拼凑后即可得到完整的代码。

这样做的好处是：所有同样的代码包（如jquery、angular）只需要下载一次，之后可以跳过所有vendor代码包的下载，大大节省传输流量。

App初次安装时也可以预置最常用的vendor代码包（如react、angular等），这样初次传输的流量也省了。

### 实现

依赖库拆分是比较困难的一件事，本文将借助webpack打包工具提供的API来进行业务代码和依赖库代码的分开构建。

首先说明整体思路：

默认构建方法中，依赖包和所有的业务代码会被打包成一个.js文件，涵盖所有代码。而现在，这个.js文件将只含有业务代码，不含有依赖包代码。这个.js文件中，所有对依赖包代码的引用会被替换成对window.$deps.[依赖包名\_依赖包版本]这样一个全局变量的引用。

接下来，通过分析npm的dependencies，调用webpack的API对每个dependency分别进行构建。并且对构建结果做转换，把构建出来的umd注册到window.$deps.[依赖包名\_依赖包版本]全局变量中。

最后，生成一个元数据文件，说明这个APP的所有依赖项，然后把构建出来的业务代码和依赖代码都上传到应用仓库服务器，就完成了APP发布的过程。

具体的实现用到了npm shrinkwrap、webpack external，可以参考“代码实现”一节中的“app-builder”。

## 根据哈希值存储依赖库或业务代码

考虑到CDN实现上的方便，本论文的设计是：不存储任何目录结构和文件之间的关联，文件只用一个哈希值唯一确定。

即构建一个Key-Value库，Key是文件的哈希值，Value是文件的内容。文件内容是业务代码、依赖库代码还是图片，这些均不关心。

APP仓库中会在MySQL数据库里维护元数据，如APP A的业务代码哈希值为a2fe71…。

有3个依赖，哈希值分别为743916…、c433b8…和71f6c3…。

获得这些数据之后，客户端可以下载对应的文件进行拼装。

这样做的好处是易于管理，利于CDN的同步，当cache miss时，可以只重新从源拉取需要的文件。

## 运行时动态拼装与链接APP

运行时，首先是下载APP的元数据，然后是通过DNS解析就近下载所有文件。

下载时注意查本地缓存，如果缓存里已经有某一个哈希代表的文件那么就不重复下载（哈希相同一定能保证文件内容相同）。

文件全部准备就绪之后，生成一个HTML文件来依次载入依赖和业务代码、同时注入getUserInfo、getUserIdentity等额外的API供应用使用。

这一步很简单，只要通过字符串拼接，在HTML源码中插入各条<script src=”…”>即可。

插入的顺序为：注入代码最先、依赖库代码其次、业务代码最后。

Web模块化的原理保证了依赖库之间代码顺序可以随意。因为每个依赖库都是自包含的，不会出现要处理依赖链路的问题，这大大简化了问题。

HTML代码生成完之后，写入一个本地的HTML文件，然后开启cordova的WebView界面并加载那个本地的HTML文件，就可以成功启动APP。

## 在NAT内部部署CDN节点

如果CDN被部署在NAT内部，那么就像内网传文件一样，速度会很快、很稳定，而且不会消耗用户任何数据流量，不产生任何费用。

本论文的设计里，通过对WIFI网关的DNS做修改、在LAN内部署APP仓库镜像，这一效果可以被达成。这样，用户可以从局域网下载App而不是从远程服务器下载，传输速度更能显著加快。

具体方案和实现请见“网络总架构设计”一章。

## 其他可以探索的技术

### brotli压缩

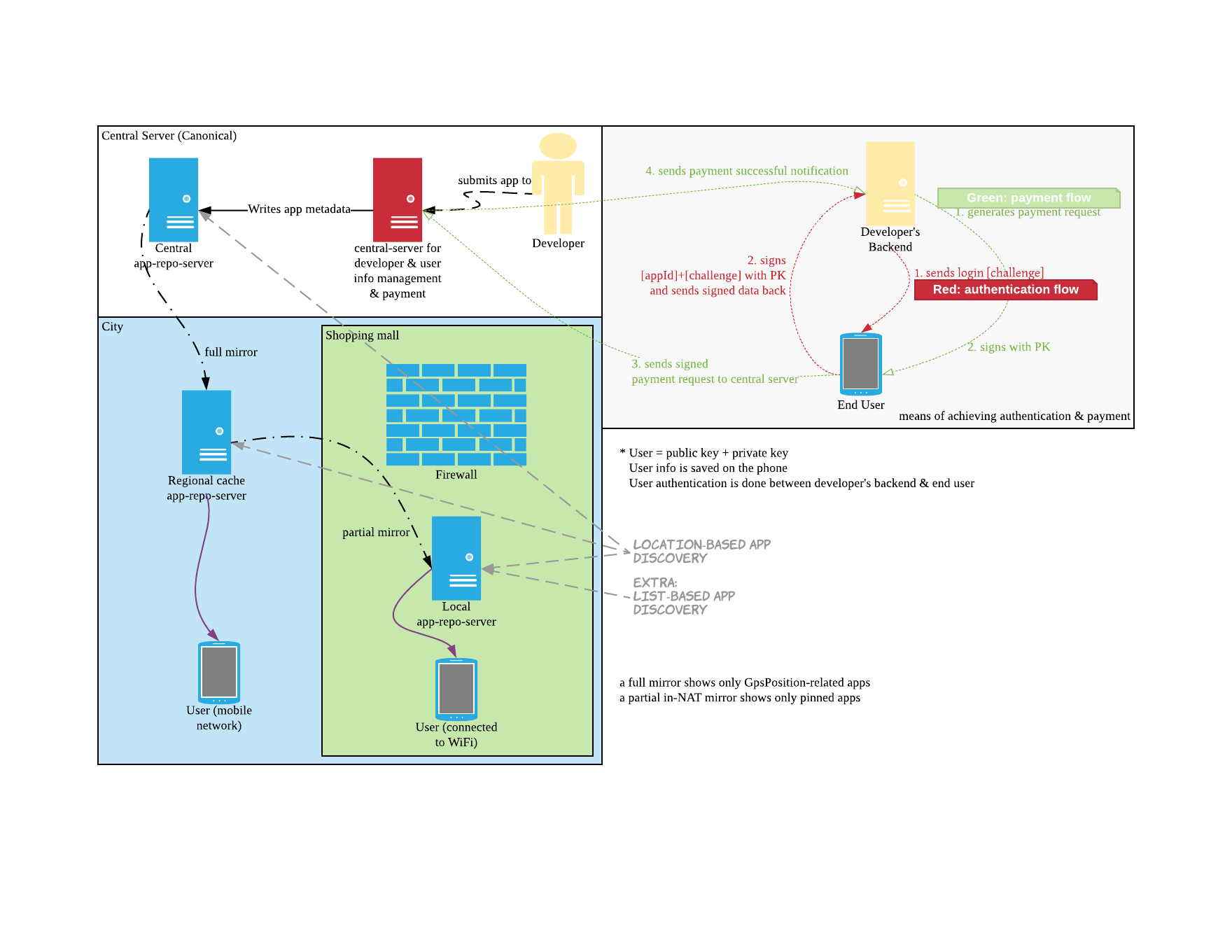
### 预先压缩

# 网络总架构设计

应用运行容器只是本论文的一小部分，更多要考虑的问题来自于网络架构和分发。

本节阐述网络架构方面的设计。

## 总架构图



如图所示，网络方面会有两种主要的服务器：数据管理服务器和应用仓库服务器。

数据管理服务器是中心化的（现阶段的设计，还是用了一些中心化服务器，更多讨论请见“完全去中心化可能性的探讨”），负责APP元数据管理、用户信息管理。

应用仓库服务器是分布式的，多副本分布在多个不同的地域（甚至在NAT内部，对于大商场而言），负责APP代码的镜像和分发。

## 主数据管理服务器

主数据管理服务器是一个中心化服务器，用来管理用户数据、APP数据、维护根据地理位置发现APP时需要使用的元数据、管理APP内支付。

开发者把构建好的应用程序包上传到主数据管理服务器，服务器会对它进行解包分析处理。会读取压缩包内的meta.json文件，以辨别APP的名称、版本、依赖项信息。随后，服务器会分别对业务代码和依赖库计算哈希并存入文件库，并在数据库中插入相应的实体数据、关联数据。同时，开发者可以设置APP发现的具体参数：在什么经度和纬度、多少米范围内可见该APP、在这个条件下启动该APP所携带的参数。这些数据会被插入到中央应用仓库服务器中，镜像自动同步工具会把这些数据同步到世界上所有别的节点（见后文），这样，APP发布就完成了。

主数据管理服务器的另一个作用是APP内支付代扣。为了方便与统一APP内的支付，本架构中不建议开发者自己接入支付服务，而是另外开发了一套基于数字签名的用户支付授权体系（见 基于数字签名的用户鉴权支付）。开发者可以在APP内调用一个统一的接口，请求用户支付，用户同意之后开发者会得到一个带有用户数字签名的支付单，需经由自己的后端转发给主服务器。主服务器就担任了验证用户数字签名、支付信息留档、联系银行转款给开发者的角色。

主服务器在现在的架构中，全世界只有一台，由一个机构专门管理。而主服务器却也有做成去中心化的可能性（见完全去中心化可能性的探讨）。如果真正上线运行，主服务器的负载是会非常大的，好在主服务器的业务都可以横向拓展。真正部署时，需使用多实例、负载均衡的方式部署主服务器。

## 应用仓库服务器

APP仓库服务器，现在的架构中有三种类型：主服务器附属应用仓库服务器（权威、唯一真相）、分布在各城市的仓库服务器、分布在各NAT内的镜像服务器。

主服务器附属应用仓库服务器在前文已经介绍过，是作为唯一真相存储和管理所有的元数据和文件，并等候别的服务器的数据同步请求（见后文）。

分布在各个城市中的服务器，相当于CDN的作用，它们的数据和主服务器完全一样（使用了镜像自动同步工具）。它们的功能就是就近分发APP、分散负载。

NAT内的镜像服务器，类似分布在各个城市中的服务器，他们把就近分发做得更进一步：只会使用内网流量。但还有一个额外的功能，就是可以通过配置的方法，提供基于LAN的APP发现的列表（即：当用户连接进这个WIFI后，主动弹出哪些APP）。

总体来说，应用仓库服务器是客户端会直接联系的服务器。客户端会把当前GPS坐标发送给服务器来进行查询，以完成基于地理位置的GPS发现。服务器的响应会是APP元数据列表，每一项都包含了APP名称、图标、主体业务代码哈希、依赖项列表和它们的哈希、启动参数等等。客户端收到这些信息后，会找出自己本地不含有的哈希，并联系应用仓库服务器进行下载。三种应用仓库服务器略有区别，却相互补充，一起完成APP发现和分发的任务。

## 镜像自动同步

分布在各城市/商场内的应用仓库服务器镜像需要定期和主应用仓库服务器进行数据同步。

数据同步主要有两方面的内容：元数据的同步，文件的同步。

元数据存储在mysql数据库中，要实现增量更新，可以通过查询updated\_at大于上次更新时间的所有记录，并把这些记录应用到本地数据库的方法来达成。这些记录中会携带文件哈希（如一个新依赖包的元数据记录会携带这个依赖包的代码哈希），如果这个哈希值对应的文件在本地不存在，则需要把它从服务器下载到本地，这就是文件的同步。以上两个步骤完成后，可以保证镜像的内容和主服务器的内容是完全一致的。

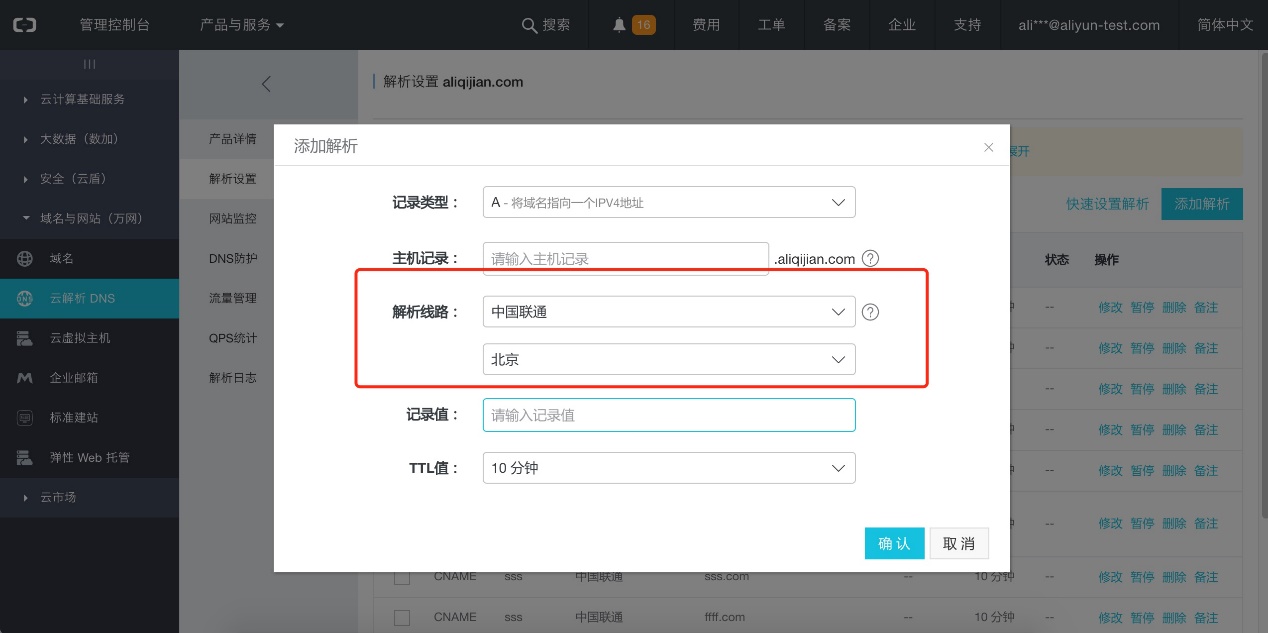
本论文使用了NodeJs来编写一个概念验证式的增量镜像同步工具，请参考“代码实现”的“mirror-tool”章节。

## 通过DNS解析进行就近分发

如前所述，在多个不同的城市部署镜像节点并就近传输，是提高网络传输效率的一个重要手段。

要能让这种方案正常运作，DNS解析服务需要做到能够按照运营商线路细分。

以阿里云提供的DNS解析服务为例，智能解析可以做到4运营商、31省份解析。有了这种解析能力，就可以设置一个统一的域名，在不同地域将它解析到那个地域下的服务器镜像上。这种改进对APP代码和用户都是透明的，却能优先使用同城内的服务器，加快速度、减少消耗。



由于DNS解析服务和多省份镜像部署都很昂贵，所以本毕业设计并没有真正做这方面的实验。

参考文献：https://help.aliyun.com/document\_detail/49060.html

## Docker容器

要支撑起这一章节所述的庞大网络架构，方便廉价的部署方案非常重要。

因为要部署的点多，所以要求要有一键部署的能力。

因为在部署NAT内应用仓库服务器时，各商场不一定愿意购置新的设备，更愿意复用旧的设备，旧设备操作系统、运行时五花八门，所以虚拟化很重要。

Docker的容器级虚拟化是解决这些问题的良好途径。我为主数据管理服务器和应用仓库服务器都制作了Docker镜像，来允许一键安装部署（见“附录：POC版本代码链接”）。

主数据管理服务器的Docker镜像中，包含主数据管理服务器和从属的应用仓库服务器，它们在安装后会自动相互协作。应用仓库服务器的Docker镜像中，包含服务器代码本身和镜像自动同步工具，同步工具已被设置好，会定时进行增量更新。如果是部署在NAT内用的，也可以改变它的配置，来达到LAN内应用发现的能力。

Docker的虚拟化屏蔽了硬件和运行时差异、提供了一键部署的能力，它的额外开销又非常小。这是一种理想的部署技术。

# 应用分发效果分析

（待补充）

## 字节传输量（使用拆分技术与不使用拆分技术）

## 传输耗时

## 移动数据流量消耗

# 基于数字签名的用户鉴权支付

以前所有App和网站都需要分开注册与登入，一人要管理很多个账号，很麻烦。

OAuth的出现较好地解决了这个问题，现在许多APP都支持“微信授权登入”、“使用QQ账号登入”，或“Sign in with Facebook / Google”。

要把体验做到极致，这种一个账号处处登入（single sign-on）的功能也必不可少。

再做一个一样的SSO系统未免比较无聊，而且我希望把系统做得尽可能的去中心化，所以我尝试了一种新的基于数字签名的用户鉴权。

## 总设计思路

用户身份的鉴别依托于非对称密钥的数字签名。这样，每个用户的身份可以由其公钥代表。

需要授权登入时，只要在本地对一个登入请求字符串（载荷）进行签名，把载荷、公钥、签名一同发送给第三方后端，在第三方后端处进行签名校验，即可以完成授权登入的行为。

这样的授权登入，无需经过中央服务器，为以后可能的进一步去中心化改造打下基础。

## 用户鉴权流程

### 前端流程

初次运行程序时，自动生成代表本用户的公钥私钥对（存储在本地私有存储区域——WebView无法访问到）。

APP内调用接口sys.getUserIdentity来进行授权请求，会弹出对话框询问用户是否答应授权。

当用户点击答应授权，系统自动生成一个登入字符串“APP:【APP名】:【时间戳】”，如“APP:car-park:1526356193580”，并使用私钥对本字符串进行签名（RSAWithSHA1）。

把私钥、登入字符串、签名一同发送给第三方后端，做身份验证。

### 后端流程

后端收到后，先验证登入字符串的内容是否合法，“APP:car-park:1526356193580”是否符合正确的格式，APP名是否正确，时间戳和当前系统时间比是否在1分钟之内。这些检查可以避免攻击者拿给别的APP的登入授权信息欺骗自己的APP，或截取到用户很多天前的一次登入授权信息后，无限次使用。

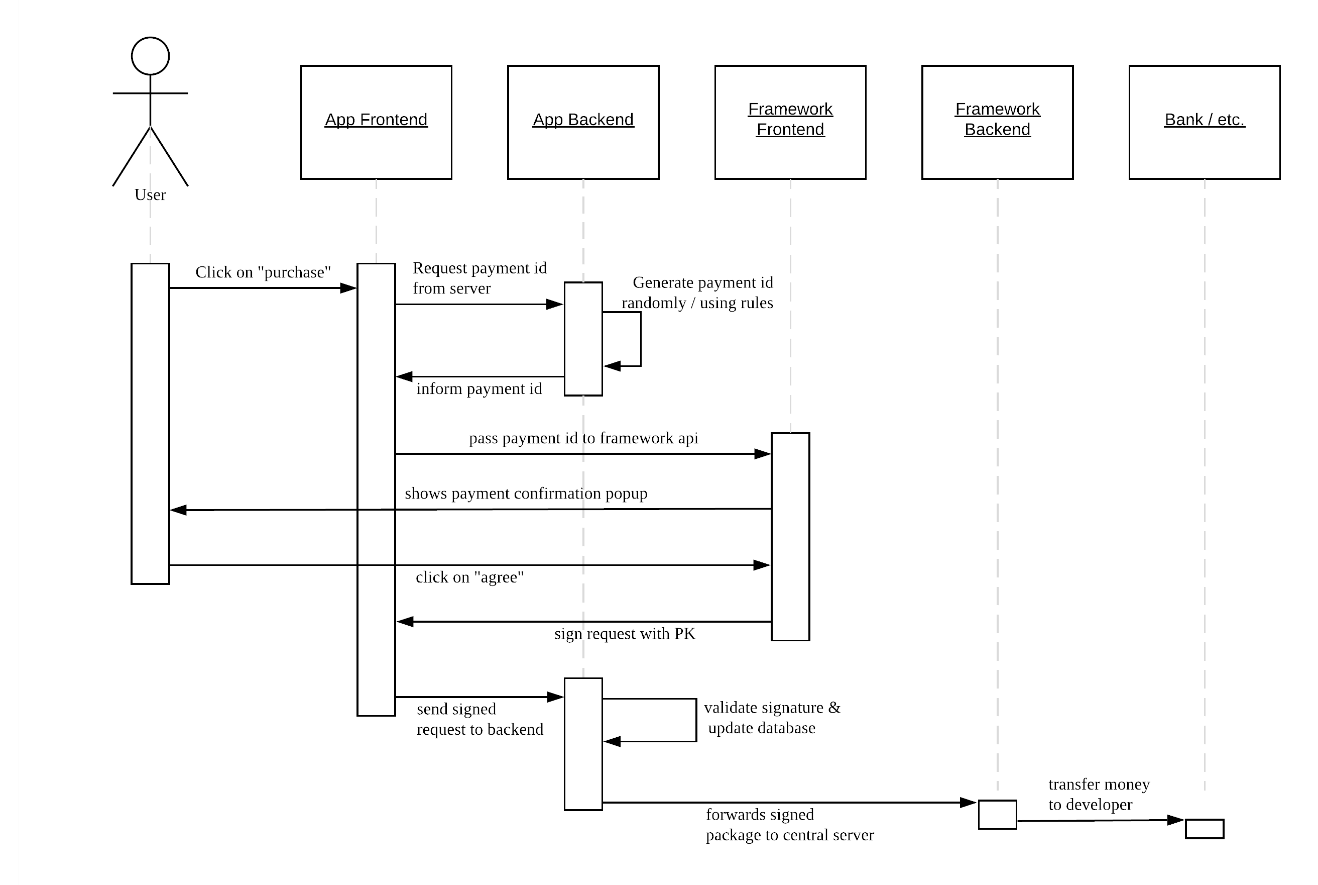
第二步要做的检查就是签名是否正确。因为只有真正的用户才有私钥，所以如果签名正确，就可以判定请求者一定是私钥的持有人——用户。

这两部判断完之后，用户的身份被成功鉴定为公钥的内容，在数据库里加一张公钥到id的转换表，就可以像普通的授权登入一样执行后续操作了。

## 用户支付流程

实现授权登入之外，本论文还要能实现便捷的付款功能，即计费支付服务也由系统代理，一键付费。付款同样可以使用数字签名的原理来进行，只是为了保证安全性、逻辑严密性，步骤会多一些。

### 支付时序图



这是付款操作的时序图，可以看到每次付款操作会有用户、APP前端、APP后端、容器前端、容器后端（本网络的中央服务器）、银行，这六方共同完成。

时序图的具体解释如下：

（待补充）

## 用户信息请求

SSO做到的是用户登入，只能用来把用户的信息确定为一个PublicKey。但这样仍然不方便，因为很多app里会需要用到用户姓名、邮箱等常用信息，用户还是得每次都填写。

为了解决这个问题，引入一个补充性的机制：用户信息请求。

这一部分其实和数字签名没什么关系，只是统一管理用户数据。比如用户姓名、用户手机号、用户邮箱地址。

在APP里可以通过一个API（sys. getUserInfo）来获得全部或部分用户数据。当然，最终用户可以选择允许或者不允许，这也是对隐私的保护。

技术实现上非常简单，只要在本地进行key、value存储，用户同意请求之后，读取value发送过去就行，不再赘述。

# 基于地理位置的服务发现

每隔一段时间从中央服务器下载附近区域的APP信息，缓存入本地数据库。

监控设备位置变化，每移动100米，从本地缓存的数据库中做查询、发现新App。

# WIFI网络内的服务发现

除了基于地理位置的服务发现，还应做WIFI网络内的服务发现。

这种情景适用于移动的物体（如列车、飞机、私家汽车）。

同时，做WIFI网络内的服务发现，更加是为了实现就近分发。当发现WIFI网络内有应用仓库服务器时，就无需走任何外网流量，而是可以直接通过局域网，把所需的APP传送到用户的手机上。

## 实现原理

DNS查询是访问任何服务的重要一环，全球只有13台根服务器，而真正做DNS查询时，不可能直接访问任何一台根服务器，因为DNS服务器有层层缓存。

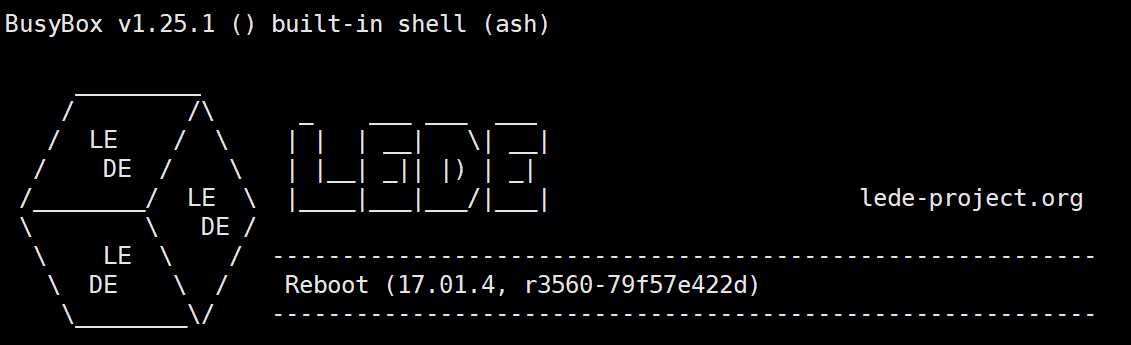
DNS缓存的特性，却反而可以用来做有意义的事情：即智能DNS、根据不同的线路给出不同的解析结果。事实上，商业上已经有很多类似的使用了，如图片CDN，虽然是同样的域名，在上海和在北京解析出的IP地址确是不同的。在上海会解析出上海的某台机器的IP地址，在北京会解析出北京的。这样可以做到透明的就近传输，加快速度、减少不必要的线路流量。

基于DNS的服务发现，有一套标准，称之为DNS-SD。（<https://www.ietf.org/rfc/rfc6763.txt>）

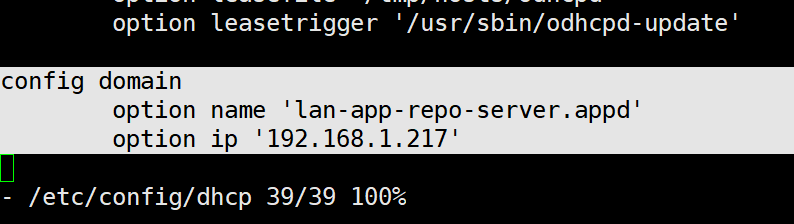
本毕业设计使用一个自创的简单版本的DNS-SD，即在路由器的DNS解析上做一些修改，让路由器能够把某个特殊的域名解析到一个内网的IP地址，达到发现的效果。

## 路由器DNS解析的配置

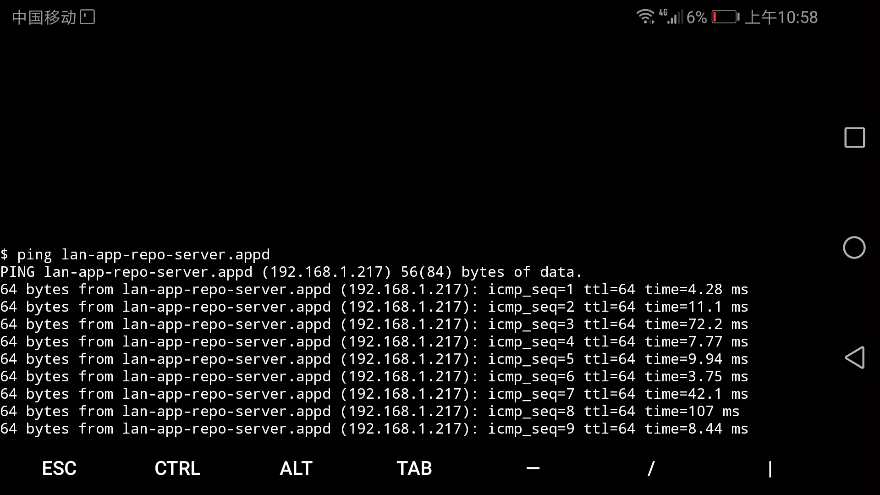
本论文尝试使用了一台装有OpenWrt (LEDE)的路由器做配置（MT7621A），



根据OpenWrt的文档（https://wiki.openwrt.org/doc/uci/dhcp），我们可以修改/etc/config/dhcp的配置，增加一行config domain的记录，即把lan-app-repo-server.appd解析到内网某台主机（比如192.168.1.217）。



应用后，连入该无线网络的手机就可以访问到专门设置的内网服务器网址。



如图所示，安卓手机成功通过DNS发现了内网服务器。发现成功后，框架会首先向该内网服务器发送LAN APP发现请求（即获得APP列表），然后，所有的文件传输请求都会先尝试经过内网服务器，当内网服务器无法提供某文件时才通过DNS解析走最近的全量服务器。通过内网传输，不仅快速，而且能帮助用户节省移动流量。

## 可能问题与解决方案

1. 从有LAN服务器的网络切换到无LAN服务器的网络，或反向切换时，如何通知程序就近下载所需文件。

解决方案：如果等要下载文件时才去判断是否为有LAN服务器的网络，势必会造成效率的降低，因此可以设计一个后台服务定期监控LAN服务器的可用性。PoC代码中，实现了LanServerAvailabilityMonitor，每隔5秒（或在安卓网络情况变化广播时）检查LAN服务器的可用性并设置标志。在要进行下载时，会根据这个标志来决定是访问LAN服务器还是访问公网服务器。如果访问LAN服务器失败，会重新从公网服务器进行下载并把标志设置为false。

1. DNS缓存会导致从一个有LAN服务器的网络切换到另一个有LAN服务器网络时，不能及时重新解析IP地址（新的网络环境下还是解析出旧网络环境下的内网IP）。

解决方案：首先，设置一个比较小的DNS TTL（比如10分钟）。局域网的DNS查询应当不会造成太高的服务器负载。  
  
然后，可以设置n个不同的域名，dns0.lan.app-discovery、dns1.lan.app-discovery、dns2.lan.app-discovery…  
依次访问，如果访问超时（即缓存了错误的IP地址），就访问下一个。  
  
总会到某一个域名，没有DNS缓存（比如dns5.lan.app-discovery），这时一个dns查询会发向路由器。  
路由器上，只要符合 /^dns(\d+).lan.app-discovery$/，都解析到同一个IP地址。

## 其他可能方案

### 端口扫描

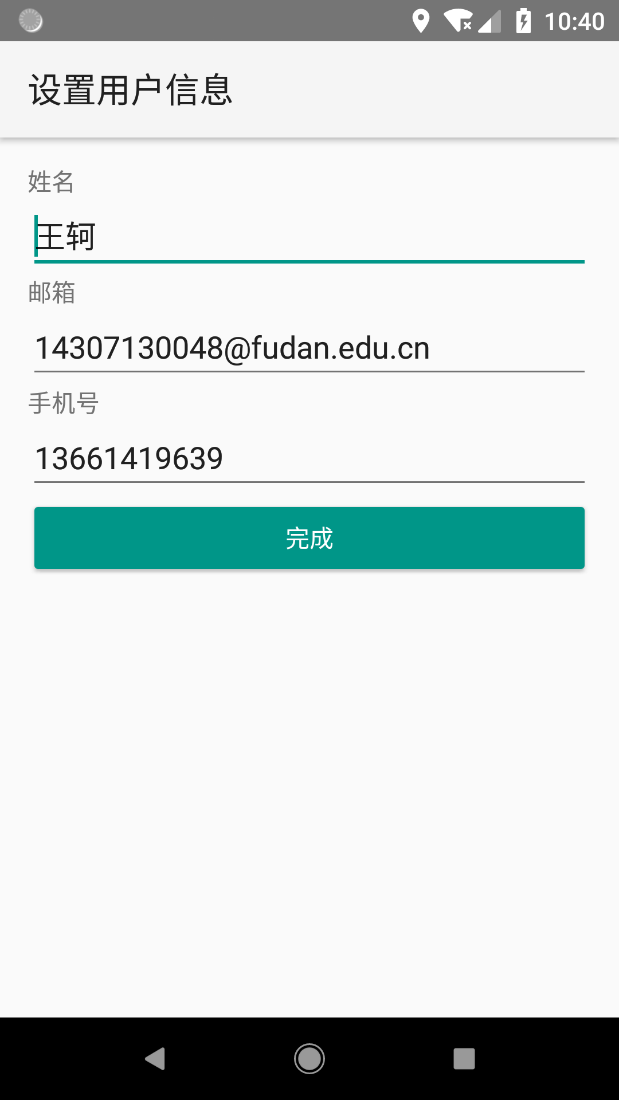
### 广播

### 默认网关上配置专属程序

# 安卓客户端的实现

## Cordova代码的改造、运行多个APP

## 用户数据的管理



目前只做了三个用户信息字段，用户可以自行设置。APP可以自由地请求这些字段中的若干个，用户也可以自由地允许/拒绝请求。

一个更加完善的用户数据管理系统，应该能支持更多类型的值设定（如车牌号等），还应该支持反向设定（如用户起初没有设置过车牌号，但是在一家停车场输入了自己的车牌号，那么这个输入的数据应自动存入用户信息字段，以后别的停车场APP就可以请求这个字段，用户无需重新输入）。这种高级的自动补全本毕业设计还没有实现。

## APP发现的实现



这是APP发现的主界面，一个列表，包含当前环境下的所有被发现的APP，点击即可使用。这个列表会综合显示基于地理位置发现的APP和基于LAN发现的APP，具体发现方法请参见对应章节。

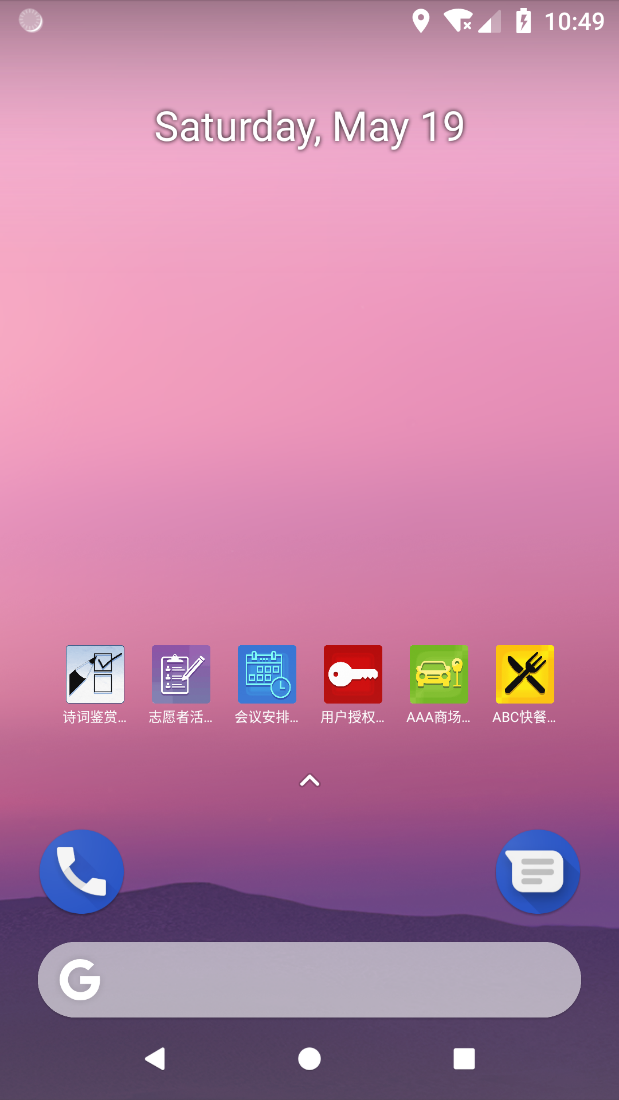
APP被发现后，会立刻进入下载队列，由于之前做过的LAN内分发和业务代码、依赖库分离，下载不会消耗多少时间，也不会消耗用户的数据流量。通常，当用户掏出手机时，APP早已下载好，可以使用。但如果APP还没有下载好，用户会得到提示，APP会在下载好的瞬间被打开。

## 本地APP代码缓存

本地APP代码的缓存非常容易，是基于哈希值的（请参考“根据哈希值存储依赖库或业务代码”章节），直接以哈希值为文件名，写入文件系统。安卓客户端中有一个统一的获取文件方法，传入哈希值，得到文件内容。它的逻辑是：先判断本地文件系统中是否有这个哈希值命名的文件，如果有，直接返回。如果没有，则从最近的网络节点根据哈希值拉取文件，写入文件系统并返回。这个过程已经达到了缓存的效果，而且缓存的时间是无限久（哈希可以直接表征文件内容）。

## 鉴权和支付的能力

## 桌面小工具



如图所示，我制作了安卓“桌面小工具”来让这些动态发现的APP看起来像已安装的APP一样，力求用户体验上的一致性。其实，这些APP图标，是桌面小工具画出来的，只是之前所展示的列表的另一种呈现方式而已。点击图标就可以像点击真实APP图标一样，弹出APP的界面。

# 拓展JavaScript能力

## 基于开源项目cordova

## 管理公钥私钥和签名

## JavaScript中调用原生接口

## 安全地弹出用户许可框

# PC运行环境的兼容处理

为了提高开发者的开发体验，本框架在PC端进行了兼容处理，即使用JavaScript的方式，实现了同样的API接口。这样，用户可以在开发机的浏览器里体验APP的整个开发流程（包括身份鉴定、信息授权、支付授权），在PC端完成开发后，开发者可以比较有信心地认为真机上运行会有一样的效果。

具体方法： （待补充）

# 应用场景探索

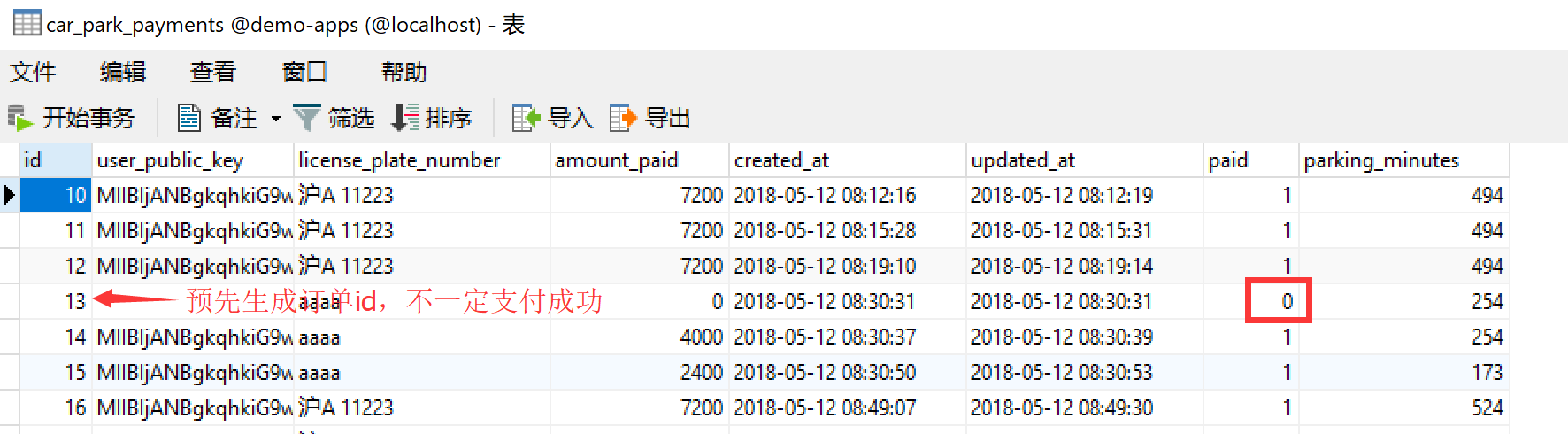
## 停车场缴费

|  |  |  |
| --- | --- | --- |
| C:\Users\Kevin\Desktop\Screenshot_1526697898.png | C:\Users\Kevin\Desktop\Screenshot_1526697895.png | C:\Users\Kevin\Desktop\Screenshot_1526697908.png |
| C:\Users\Kevin\Desktop\Screenshot_1526697914.png |  |  |

这个DEMO同时涉及到读取启动参数（获得停车场ID）、请求用户身份、请求APP内支付等功能，有一个独立的后端，实现了支付时序图的完整流程。

支付框弹出之前，会请求停车场缴费APP的后端生成订单号（数据库会记录订单应付金额、订单内容，并把“已付款”设置为false）。

前端会根据这个后端返回的订单号请求支付，用户同意后进行签名，发回给后端，后端随即把“已付款”设置为true。



如图，这是停车场缴费程序后端的数据库，有些记录“已付款”为true，有些记录“已付款”为false（虽然向后端请求了支付，但并没有发支付授权签名给后端。是因为用户拒绝了支付请求）。

后端验证完支付授权签名之后，会把支付签名转发给中央服务器。中央服务器随即会验证支付授权签名，在验证通过之后，调用银行转账的接口把费用转给

开发者。



如图，这个界面是中央服务器统计的支付记录，各种APP的成功支付都会被中央服务器记录。

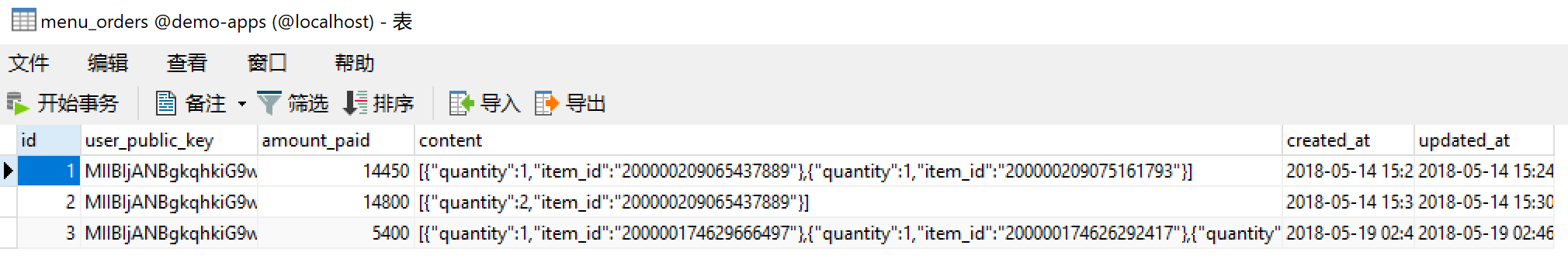
## 餐厅点菜

|  |  |  |
| --- | --- | --- |
| Screenshot_1526697941 | Screenshot_1526697955 | C:\Users\Kevin\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Screenshot_1526697968.png |

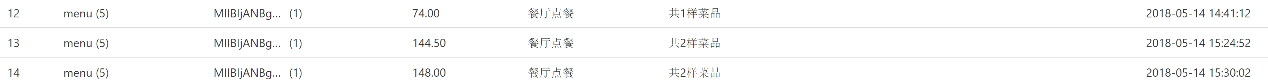
这是一个很有商业价值的场景。实现的内容和现在已经存在的扫码点菜比较类似。

用户点击APP即可点菜、下单、在线支付。这个DEMO在用到的技术上和“停车场缴费”类似。

用户同意支付之后，支付授权签名同样会被发给点菜应用的后端（后端可以通知服务员做菜），后端同样会把它转发给中央服务器，以真正实现收款。



如图，这是餐厅点单后端的数据库，可以记录用户已付款的信息和用户的订单内容。



这是中央服务器收到的支付记录，这些记录里的金额是最终可以结算给商户的。

## 在线考试

|  |  |  |
| --- | --- | --- |
| C:\Users\Kevin\Desktop\Screenshot_1526697671.png | C:\Users\Kevin\Desktop\Screenshot_1526697711.png | C:\Users\Kevin\Desktop\Screenshot_1526697717.png |
| C:\Users\Kevin\Desktop\Screenshot_1526697753.png | C:\Users\Kevin\Desktop\Screenshot_1526697763.png |  |

这个应用场景可以允许老师给教室里的学生推送随堂测试考卷。学生点击桌面上的APP进入考试界面。

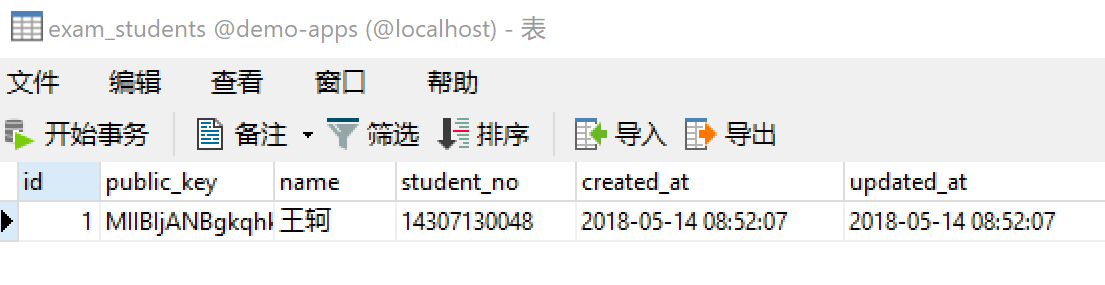
第一次进入考试界面后，需要完善个人信息（即姓名、学号），这些信息会被发送到后端，和用户的publicKey做关联，那么以后每次API请求，都可以知道是哪个学生发送的请求。

随后，有一个等待考试开始的环节，考试可以在老师的操控下同时开始，并设置持续时间。时间到后自动收卷、在线批改统计分数、并记录到数据库。

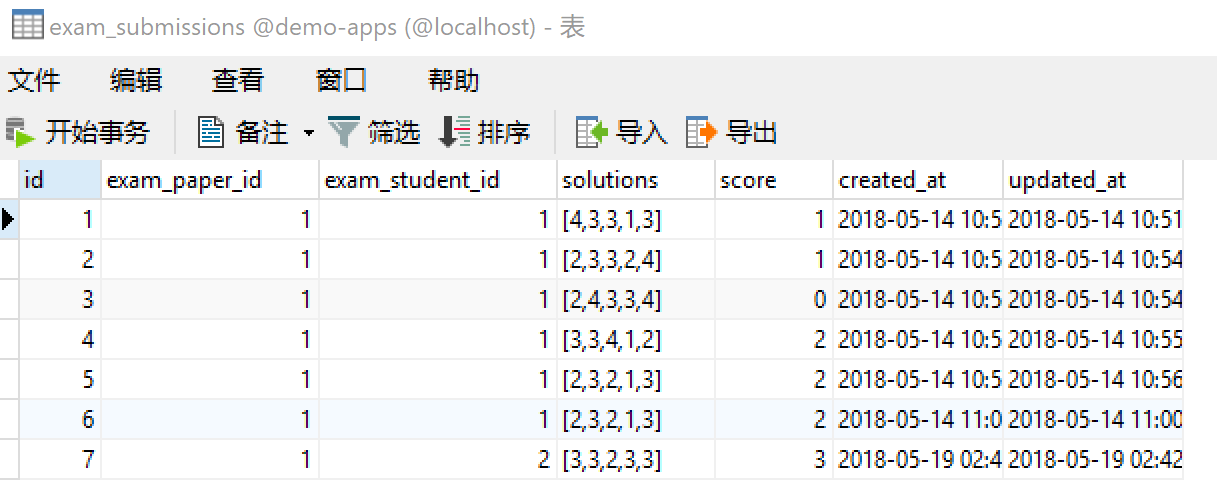
因为参与考试者的身份是公钥+数字签名，APP也是根据环境推送的，所以在一定程度上，可以加大代考的技术难度。（若要代考，则必须获得对方的privateKey / 修改客户端代码后请对方人工做数字签名 / 或直接把对方的手机拿到教室）



这是在线考试后端的试卷数据库，题目和答案使用json来定义（json被发送给学生时，会被抹去“答案”字段——“答案”只在在线批改时被使用）。is\_enabled是个布尔值，代表试卷是否被推送给学生。考试开始时，会从false被设置为true，客户端那边会轮询，当变为true时，后端会从返回“等待考试开始”变为返回试卷内容。allowed\_time\_seconds是考试持续时间（秒），超过这个时间后前端会强制自动交卷（后端也可以设置为：超过这个时间若干秒后，不再接受交卷）。



这是数据库里存储学生信息的表，公钥和学生信息通过这张表建立关联。



这是考试提交记录的表，可以看到学生的回答和系统自动计算出的得分。

## 会议时刻表

|  |  |  |
| --- | --- | --- |
| C:\Users\Kevin\Desktop\Screenshot_1526698615.png | C:\Users\Kevin\Desktop\Screenshot_1526698620.png |  |

这个DEMO APP比较简单，是会议室应用场景的探索。

用户进入会议室之后，手机上可以直接弹出会议安排APP，点击即可查询每个子会议室的日程安排（讲座时间、讲座内容、主讲人）。

更多的带有和参会人交互的功能也可以被加入本APP。

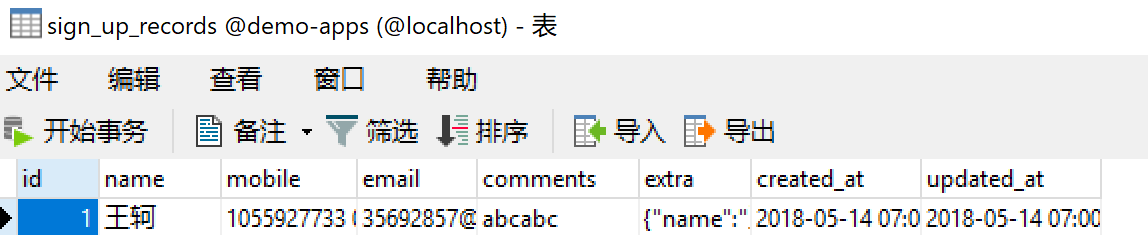
## 活动报名

|  |  |  |
| --- | --- | --- |
| C:\Users\Kevin\Desktop\Screenshot_1526697803.png | C:\Users\Kevin\Desktop\Screenshot_1526697809.png |  |

这也是一个简单的DEMO APP、用来下发活动报名表单。

用户点击APP即可报名活动。表单的部分字段使用用户信息请求的机制自动帮用户填写，以省力。

这种场景尤其合适社团摆摊招募。同学希望参加社团活动时，可以直接掏出手机报名活动。



报名记录直接被保存进后端数据库。

## 应用场景的总结、畅想与商业可能

以上是我为了挖掘潜在应用场景，自己制作的5个迷你app。之前还设想过博物馆导览、智能家电控制面板、智能私家车车载系统等等。但时间和硬件方面的因素并未完成。

应用场景初步看来是两方面的，一方面是为商户提供服务（广义的商户也包括会议举办方、社团等），另一方面是为用户本身提供服务（智能家电、远程控制）。

为商户提供服务方面，许多和环境有关的APP，业务都高度相似。它们有许多共同流程、共同的组件，所以开发者（或开源社区/项目外包公司）可以制作一个高度发达的通用组件库。之后写常见的程序，只要配置组件就行。

这样就可以以极其低廉的价格给每个停车场、商铺定制APP。客户不花很多钱就得到品牌形象的提升、业务更加便捷；定制方不费很多力就得到了报酬。这种模式有良好的潜在商机。

为用户本身提供服务方面，也有很多深度可以挖掘。比如，当用户进入自己的私家车后，手机自动出现私家车APP，可以在APP里实时监控车的状态、油耗，调节座椅、天窗、空调，甚至导航、播放音乐；回家之后，可以点击自动弹出的智能家电APP，开灯关灯、开电视机调频道…具备这些智能功能的硬件，能更让用户享受到科技带来的便捷，得到用户青睐。这成就了一种连接一切的可能性，更棒的是，因为所有设备都遵循统一开放的APP发现协议，所以一切都是免配置的——进房即用。

为商户提供服务主要会用到基于地理位置的APP发现；而为用户本身提供服务主要会用到局域网内APP发现。两种发现原理不同，互为补充，都可以照料到。

# 完全去中心化可能性的探讨

本毕业设计的架构里，还是用到了中央服务器这一个概念，没有完全去中心化。即还是会有一个机构（类似ICANN）来管理这一整套系统。如果能做到完全去中心化，那么这套技术架构和协议会更加开放、对所有人更加公平。

目前中央服务器存在的主要意义在于：APP元数据的管理、根据地理位置发现APP所用数据的维护、管理APP内支付、抑制诈骗类APP。可以认为，在目前的这个架构下，只有一份真相（就像13台根DNS服务器一样），所有的子节点都是从根服务器同步数据（或在LAN发现APP的情况下，轻微添加一些额外数据）。

如果要去掉中央服务器，需要解决上述所说的几个问题。

APP内支付问题应该是最容易解决的，现在的模式是中央服务器代扣代收，但完全可以和银行、支付宝等进行合作，添加一种基于数字签名的支付。即：把用户公钥和银行卡/支付宝进行关联，用户签署一笔支付请求后，直接把签名发给银行/支付宝，商户直接收到来自银行的付款通知。

APP元数据管理、地理位置数据维护，稍微有一些艰难，因为没有了中央服务器，信息的发布成为了一个问题。但我们可以参考已有的纯P2P网络，比如：比特币、freenet，用类似的方法解决问题。这些解决方案主要是基于广播，发布数据时像病毒传播一样，一传十十传百。理论上这种网络是可以支撑整个方案，代替现在的中心化APP仓库服务器的，但是这对每个节点的硬盘容量、网络质量、节点密布数产生了比较大的要求。发布新版本APP的速度可能会变慢（新数据可能要很长时间才会被发布到全球各个节点），APP初次启动时间也会非常长（初次启动时需要通过盲目的搜索，搜到一台节点，才可以用它来进行APP发现——或许也可以参考BT下载中PEX节点交换的技术，即始终跟路由器交换已知节点列表，来加速初次启动的发现过程）。

信用问题（诈骗APP防范），看似难解，实际却也有解决思路。可以参考https证书（EV）的思路，交给可信第三方来解决。即一个第三方机构（如VeriSign）调查你的资质（上海XX商业广场），调查成功后，用他们的公钥给你的APP签名（上海XX商业广场地下车库缴费程序）。因为可信第三方的公钥是预先录在系统里的，所以通过这个签名，用户就可以得知：即将打开的APP的确是上海XX商业广场所颁发的，至少，可信第三方已经帮你调查过APP发布者的身份了。

可能最难解决的问题，反而是APP膨胀的问题。即什么样的人到最后都想发APP，然后广告类型的APP遍地都是。这个问题需要采用综合手段来解决，一种可以探索的思路是：引入用户评价体系。即用户使用后可以询问该APP是什么类型的（广告/商店/便利服务/咨询），顶还是踩。用户的反馈同样会被签名，分发到各个节点中。节点会在客户端请求发现APP的同时把投票的统计数据一并返回给客户端，客户端上可以设置过滤和筛选条件。

但如何保证不法分子不会生成几十万个密钥对，对想要推广的APP进行投票，来混淆视听呢？一种方法是网络实名制，即像身份证一样，每个人只能拥有一个公钥私钥对（或者说他的公钥本身就是被签过名的）。

更可行的方法是“自由选择信任对象”，建立起多个非盈利组织，这些组织里的人帮助最终用户甄别是非、维护判断未知APP属性的数据。这些组织各有自己的公钥，他们对APP进行的投票才是客户端真正关心的投票。用户到底信任哪些组织（哪些公钥），这是可以让用户自己设置的。如果用户发现应用A明明是个广告，组织a却投票说A是个咨询APP，那么用户可以把对组织a的信任给移除，组织b、组织c会给正确的投票。久而久之每个信任组织会有自己的口碑评价，也会珍惜自己的权力。

另一种简单的方法，增加可信第三方认证的收费即可。如果发布一个带签名的APP需要投入较高的成本，那么广告类APP就不会发得那么猖狂。对于学校等不能支付高昂费用的机构，可以引入“可选择相信的第三方”，即默认不相信学校公钥签发的APP，但学生可以手动勾选相信。勾选完之后，所有学校公钥签发的APP和支付高昂费用后请专业第三方信任机构签发的APP有同等地位。

通过以上的分析，我初步认为一个完全去中心化的版本是有可能可以做的。但有许多细节需要进一步探讨、各种协议的制定和实现也将是一个工程上的巨大挑战。

# 附录：PoC版本代码链接

一个可以运行的POC版本已经发布到GitHub上。

<https://github.com/environment-based-app-discovery-KW/>

有以下几个git仓库：

## design

设计相关文档

## demo-apps

DEMO APPS，包含停车场缴费、餐厅点单、在线考试、会议日程表、活动报名五个APP，旨在探索本技术适用的场景、并提供本框架上的前后端开发DEMO。

## app-builder

基于webpack的app前端构建器，能够打包出vendor分离的代码包。

## app-repo-server

APP仓库服务器，分布式多地部署（可在NAT内部署），存储与管理app代码、元数据、部署信息。

## android-app

安卓客户端：本地拼装APP、缓存依赖、提供用户信息获得/鉴权/支付的JavaScript接口、桌面小工具快速启动APP。

## app-auth-demo

用户鉴权、获得用户信息、支付的前端API的DEMO。

## central-server

中央服务器，用来管理用户数据、上传新APP（写入app-repo-server）、管理APP内支付。

## mirror-tool

app-repo-server的同步工具，可以用来定时同步最新依赖库和APP的代码。

# 总结

本毕业设计探索了一种新的APP范式，从哲学层面对它进行了构思，并深度挖掘了技术上可能遇到的各种挑战，创新性地给出了解决方式。此外，本毕业设计还从商业应用的角度对这种新范式可以带来的可能性进行了探索。

在实现层面，本APP完成了一个概念验证：构建起了APP中央服务器和分布式APP仓库服务器网络，实现了数据同步、NAT内分发；实现了基于地理位置的APP发现和基于LAN的APP发现；实现了构建时依赖库与内核代码拆分、运行时动态拼装以节省流量；实现了一个安卓客户端、以桌面小工具的方式模拟了主动发现后弹出的APP；实现了用户信息授权和支付流程…

本毕业设计还探讨了完全去中心化的可能性，它涉及到一种分布式信任系统的设计。完全去中心化，是这类系统的最终目标、终极升华，是做开放标准架构的证明。这也是本毕业设计和微信小程序哲学上的不同点。

在本毕业设计的最终可能形态里，这种技术可以被植入安卓和iOS系统本身，并成为人们使用手机的一种习惯，而世界各个角落的骨干网络、商场WIFI里，都有分布式的分发节点（已经被做成了完全去中心化的架构）。它在商业上中性独立，却能给使用者和商户同等地创造价值。

这个目标非常宏大，当然不是我的毕业设计可以企及的，但我非常希望我毕业设计的探索可以启发一些标准制定机构做这件事情，并把人们使用手机APP的方式推向下一个阶段。

# 致谢

# 参考文献

（参考文献待补充）