天津大学

安卓 APP 权限分析平台项目报告书

学　　院　国际工程师　学院

年　　级　2018　级

姓　　名　后永胜 2018229035

姓　　名　刘懿 2018229042

姓　　名　袁莎莎 2018229054

2019 年 11 月 23 日

项目分工：

后永胜：数据分析及项目数据库设计与实现

刘懿：权限解析工具设计，推荐系统功能设计

袁莎莎：主体功能设计，测试计划设计

目录

第一章 绪论

1.1 课题背景及意义

随着移动互联网的快速发展和各类应用程序的应运而生，手机逐渐成为用户连接网络和存储个人信息最重要的设备，在人们生活中处于越来越重要的地位。Android 应用程序的多样性同样吸引了越来越多的用户开始尝试并使用 Android 系统的智能手机。在人们对高端和大屏幕移动设备的需求以及 5G 的应用和普及下，全球智能手机的需求将大幅增加。根据国际数据公司全球季度手机追踪系统的数据统计，自 2017 年第三季度起，全球智能手机 99.9%都是基于 Android 系统和 iOS 系统的，并且基于 Android 平台的智能手机份额徘徊在 85%左右。与此同时，Android 系统的开放性吸引了更多的应用程序开发者，第三方应用程序开发人员可将应用程序上传到市场并发布到大量移动设备终端，使得应用程序数量迅猛增加。各种功能应用程序大量涌现，在满足了用户的需求的同时，为了迎合用户的喜好而采集用户的私人数据和行为习惯的现象早已司空见惯。

Android 应用开发者的过度申请权限、APP 利用权限漏洞而提升权限和第三方应用市场不完善的审核机制等，使得 Android 软件大量存在权限泄露等问题。由此可见，Android 采用的权限机制对用户数据安全性进行保护的方法并不能达到理想的安全防御效果。在这样的情况下，如何高效地对 Android 应用程序权限使用情况进行分析以及保护用户隐私信息已经成为一项研究重点。

1.2 系统目的

通常我们手机中的 APP 会向用户获取很多权限，这些权限有些涉及个人隐私。大多数 APP 在安装、更新时，都会向用户申请获取相关手机权限，而摄像头、麦克风、通话、短信等涉及用户个人隐私的敏感权限尤为突出，甚至一些与此无关的 APP 也要求获得此类权限。

如果因为开了某些不必要的权限，我们的个人数据可能每时每刻都面临着窃取的风险。用户在安装 APP 时，可以对权限进行设置，设置过多的权限，不利于用户对应用程序进行把控，应用程序可以在不通知用户的情况习使用隐私信息，

威胁用户的安全和隐私；而设置过少的权限，会带来复杂的操作，影响用户的体验。如何选择开取软件相关权限，使得我们既能正常的使用 APP 提供的功能，又能降低个人数据泄露的风险，成为了亟须解决的问题。本项目旨在通过分析大量用户对权限的设定行为，为用户提供权限设定方案。

第二章 技术简介

2.1 程序设计语言 Python

Python 是一种跨平台的计算机程序设计语言。是一种面向对象的动态类型语言，最初被设计用于编写自动化脚本(shell)，随着版本的不断更新和语言新功能的添加，越来越多被用于独立的、大型项目的开发。它经常被应用于 Web 和 Internet 开发、科学计算和统计、人工智能、教育、桌面界面开发、软件开发和后端开发等多个领域。

Python 在设计上坚持了清晰划一的风格，这使得 Python 成为一门易读、易维护，并且被大量用户所欢迎的、用途广泛的语言。在使用 Python 设计程序时，设计者开发时总的指导思想是，对于一个特定的问题，只要有一种最好的方法来解决就好了，这也使得 Python 在得到了越来越多的重视和应用。

2.2 编译工具 APKTool

APKTool 是 GOOGLE 提供的 Android 应用程序包（APK）编译工具，能够反编译及回编译 APK，同时安装反编译系统 APK 所需要的 framework-res 框架，清理上次反编译文件夹等功能。其具体功能有：

1) 将资源解码成原来的形式（包括 resources.arsc，class.dex，9.png 和 xml）
2) 将解码的资源重新打包成 APK/jar
3) 组织和处理依赖于框架资源的 APK
4) Smali 调试
5) 执行自动化任务

2.3 深度学习

深度学习（DL, Deep Learning）是机器学习（ML, Machine Learning）领域中一个新的研究方向。

深度学习是学习样本数据的内在规律和表示层次，这些学习过程中获得的信息对诸如文字，图像和声音等数据的解释有很大的帮助。它的最终目标是让机器能够像人一样具有分析学习能力，能够识别文字、图像和声音等数据。深度学习在搜索技术，数据挖掘，机器学习，机器翻译，自然语言处理，多媒体学习，语音，推荐和个性化技术，以及其他相关领域都取得了很多成果。深度学习使机器模仿视听和思考等人类的活动，解决了很多复杂的模式识别难题，使得人工智能相关技术取得了很大进步。

再利用深度学习的过程中，我们通过设计建立适量的神经元计算节点和多层运算层次结构，选择合适的输人层和输出层，通过网络的学习和调优，建立起从输入到输出的函数关系，虽然不能 100%找到输入与输出的函数关系，但是可以尽可能的逼近现实的关联关系。使用训练成功的网络模型，就可以实现我们对复杂事务处理的自动化要求。

2.4 推荐系统

推荐系统是根据用户的信息需求、兴趣等，将用户感兴趣的信息、产品等推荐给用户的个性化信息的系统。推荐系统通过研究用户的兴趣偏好，进行个性化计算，由系统发现用户的兴趣点，从而引导用户发现自己的信息需求。一个好的推荐系统不仅能为用户提供个性化的服务，还能和用户之间建立密切关系，让用户对推荐产生依赖。

推荐系统现已广泛应用于很多领域，其中最典型并具有良好的发展和应用前景的领域就是电子商务领域。同时学术界对推荐系统的研究热度一直很高，逐步形成了一门独立的学科。

推荐系统有 3 个重要的模块：用户建模模块、推荐对象建模模块、推荐算法模块。通用的推荐系统模型流程如图。推荐系统把用户模型中兴趣需求信息和推荐对象模型中的特征信息匹配，同时使用相应的推荐算法进行计算筛选，找到用户可能感兴趣的推荐对象，然后推荐给用户。

2.5 图数据库

Neo4j 是由 java 实现的开源 NOSQL 图数据库，它可以将结构化数据存储在网络上。使用图数据库可以方便的建成一个庞大的用户关系网，进而分析用户的不同的权限设计行为，通过分析这些不同的设计行为，来为相近用户推荐权限设置的方法。Neo4j 图数据库村粗的庞大的关系网可以为我们的推荐系统设计提供数据支撑。

2.6 可视化工具

Seaborn 是一个用 Python 制作统计图形的库。它建立在 matplotlib 之上，并与 pandas 数据结构紧密集成。Seaborn 旨在使可视化成为探索和理解数据的核心部分。其面向数据集的绘图功能对包含整个数据集的数据框和数组进行操作，并在内部执行必要的语义映射和统计聚合，以生成信息图。Seaborn 面向数据集的 API，用于检查多个变量之间的关系；专门支持使用分类变量来显示观察结果或汇总统计数据；可视化单变量或双变量分布以及在数据子集之间进行比较的选项；不同种类因变量的线性回归模型的自动估计和绘图；方便地查看复杂数据集的整体结构；用于构建多绘图网格的高级抽象，可让您轻松构建复杂的可视化；简洁的控制 matplotlib 图形样式与几个内置主题；用于选择调色板的工具，可以忠实地显示数据中的模式。

Seaborn 可以很方便的分析数据之间的关系，作图既简便有美观，对于项目中的数据分析展示有很大作用。

2.7 权限机制

权限机制是 Android 系统保护用户安全和隐私的重要机制。Android 通过权限机制限制应用程序对系统资源和用户数据的访问，以及敏感操作的执行。应用程序若需要访问系统资源和用户数据，则必须在 AndroidManifest.xml 文件中明确声明相关的权限。在 Android 6.0 之前，用户在安装应用程序时决定应用能或不能获得所申请的所有权限。Android 6.0 之后，采取了运行时权限机制。在应用程序运行阶段，当需要某个权限组的权限时，应用程序动态向用户进行弹框申请，如果用户同意，则权限组包含的所有权限被打包赋予给应用程序;如果用户不同意，则不授予权限。用户也可以在系统设置中对权限组进行设置，系统将应

用程序使用的权限组全部列出，用户可以逐一对权限组的设置选项选择打开或者关闭，设置打开，则将权限组的权限赋予应用程序，应用程序可以随时使用这些权限组而不需要申请;选择关闭，则应用程序需要用到这些权限组的权限时，需要向用户动态申请。

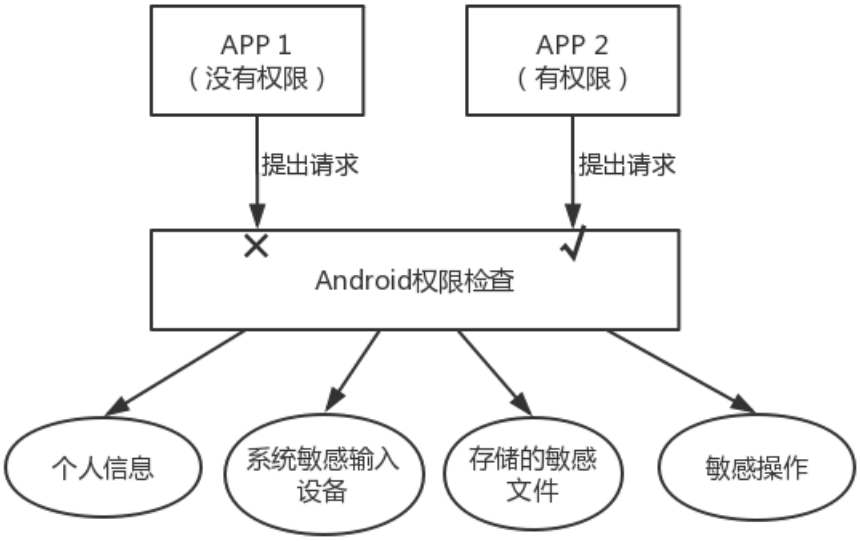

图 1 Android 权限检查

Android 通过权限机制保护资源。Android 系统会根据清单文件和用户的授权制定应用程序的权限规则，当应用程序想要访问敏感资源时，Android 系统会检查应用是否具有相应的权限，具体步骤如图 1 所示。在同一个应用程序中的所有组件拥有相同的权限。现在 Android 系统提供了超过 150 个权限来保护从框架层到系统层的各种资源。在框架级别，Android 提供特定于设备的系统服务，如电话、位置和摄像头，以及各种内容提供者，如联系人、通话记录和短信。在操作系统级别，系统资源通过 Linux 安全机制进行管理，例如文件系统和网络套接字的 Unix 权限。

第三章 需求分析

3.1 功能需求

在本系统中用户为手机用户，用户手机中有大量的软件，这些软件需要不同的权限，用户对如何正确的设计相应的权限比较伤脑筋。本系统主要为这些用户提供软件权限设置方案，同时也需要开放的社区系统，供大家交流一些经验；良好的交友系统，通过观察朋友们如何设置权限来设置自己的权限；强大的推荐系统，通过收集大量用户权限设置行为，为用户提供权限设置方案。

3.2 可行性分析

权限提取：我们可以利用 APK 逆向编译工具 APKtool 将 APK 软件包中的权限设置文件提取出来；

图数据库：Neo4j 图数据库可以以图的形式存放大量用户的权限信息，这为我们的推荐系统部分设计提供了大量的数据支撑；

推荐系统：使用机器深度学习的推荐系统与传统机遇协同过滤的推荐系统结合，以及图数据库中的用户关系数据支撑，这为我们为用户提供不同 APK 的权限设计方式提供了方法支撑；

3.2.1 数据来源

我们可以在网站上下载 APK，每个 APK 文件内包含被编译的代码文件(.dex 文件)、文件资源、原生资源文件、证书以及清单文件。

3.2.2 权限获取

首先我们使用 Google 提供的权限解析工具 APKTool 对获得的 APK 包进行反编译，得到生成目录中 APK 的配置文件 AndroiManifest.xml，其标记着 APP 安装时需要开启的权限信息。其次，我们使用 Python，将文件中的权限信息提取出来，并且只保留 APP 所请求权限的名称信息。

3.2.3 权限推荐

我们使用机器深度学习的推荐系统与传统机遇协同过滤的推荐系统结合，对用户进行 APP 权限信息的推荐。

3.3 用例分析

3.3.1 用户管理用例

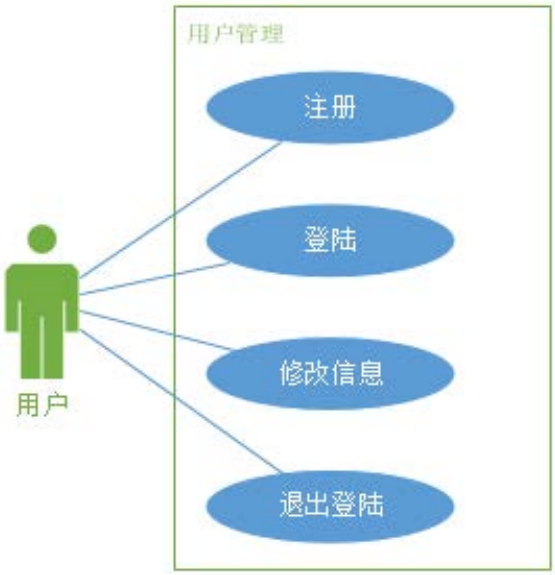

图 2 用户管理用例

针对用户来说，用户需要注册账号以使用本系统。用户在注册账号之后，可以用本人注册的账号登陆系统，并可进行修改信息、登出等操作。

3.3.2 APK 权限管理用例

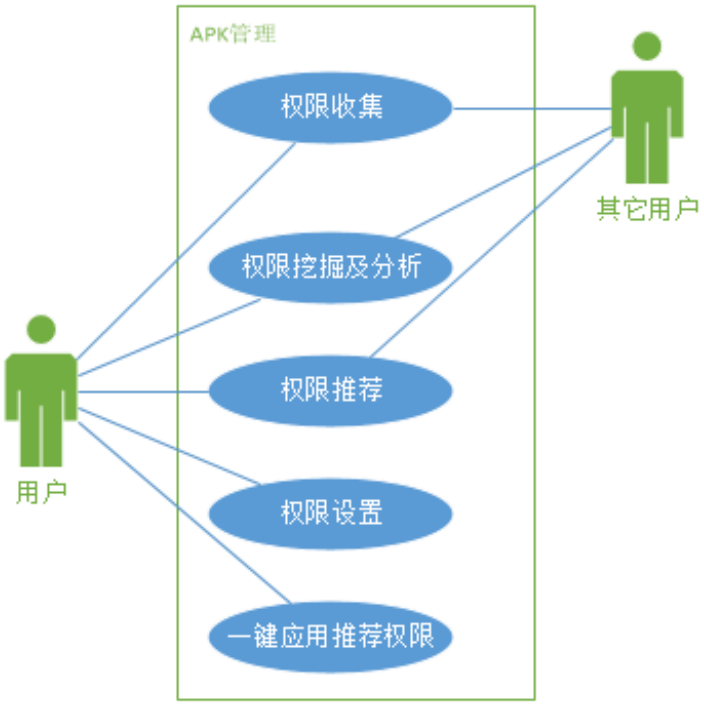

图 3 APK 权限管理用例

用户在登陆系统之后，可以利用系统中的 APK 权限分析工具对 APP 的权限进行挖掘和分析，并通过系统中的权限推荐系统获得 APP 应开启权限的推荐。用户可以自行对权限进行设置，也可根据系统推荐的权限对 APP 所开启的权限进行一键设置。

同时，用户对 APP 的权限设置会被记录并上传数据库，并通过相关推荐算法推荐给社区中的其他用户。

3.3.3 社区管理用例

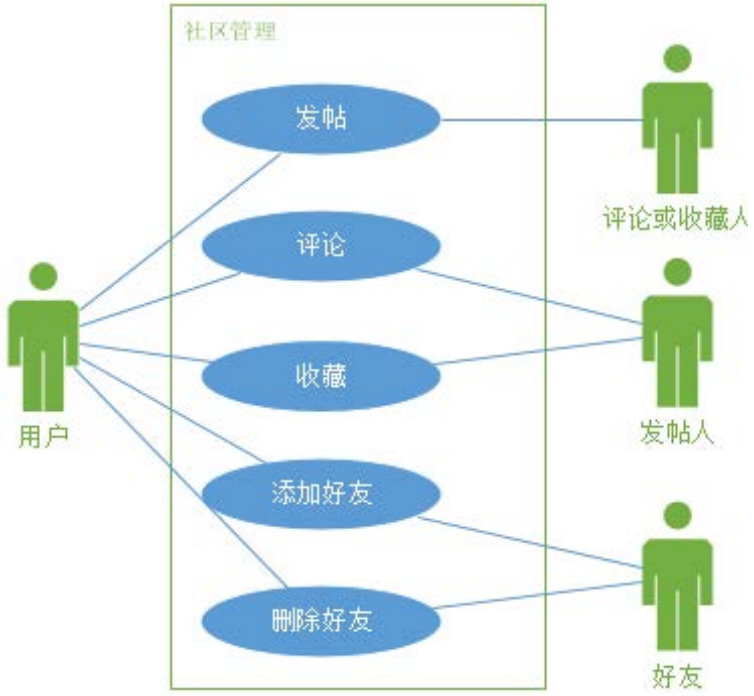

图 4 社区管理用例

用户在登陆后，可以在社区中通过发帖、评论等与社区中的其他用户进行交流。同时，用户可以对其他用户的帖子进行收藏。用户可以添加、删除好友，以方便与其他用户的交流。

第四章 概要设计

4.1 总体功能设计

本项目的权限分析平台主要由 APK 权限管理、用户管理和社区管理三部分组成，如图 5 所示。

图 5 APP 权限分析平台功能需求

APK 权限管理部分主要是对 APK 的管理，首先对 Android 应用程序包进行收集；其次使用 APK 编译工具和 python 程序对权限进行挖掘和分析，得到该应用程序在用户安装时所需要获取的权限信息；然后根据收集到的权限信息，对用户安装的其他 APP，所需要开的权限进行推荐，为用户提供权限设定方案；用户可以根据本系统推荐的权限对 APP 开启的权限进行一键设置，也可以自己对权限进行设置。

用户管理部分主要分为账户管理和基本信息管理。在使用本系统之前，用户需要先填写个人信息进行注册；用户登录之后，可以使用本系统，并且可以对自己的基本信息进行修改。

社区管理部分主要分为发帖管理、评论管理以及好友管理。用户在登录之后，可以发帖，以及对其他人的帖子进行评论；可以提出新的 APP 权限信息以及对系

统推荐的权限进行反馈，以使系统的推荐更准确；用户也可以进行添加和删除好友操作，以便和其他用户交流。

4.2 数据库总体设计

数据库系统采用图数据库 neo4j，主要有如下三个关系：

关系一：(apk) -[:require]-> (permission)

关系二：(user) -[:use]-> (apk) -[:allow]-> (permission)

关系三：(user1) -[:friend]- (user2)

关系一表示 APK 需要哪些权限；关系二表示，用户用了哪些 APK，对这些 APK 允许了哪些权限；关系三表示用户与用户之间好友的关系。

第五章 详细设计

5.1 权限解析工具设计

权限解析工具的主要功能为读入一个或多个 APP 的 APK 文件，输出该 APP 在安装时所请求开启的权限列表。

本权限解析工具使用 APKTool 中的 APKtool d <file.APK> <dir> 命令对应用的 APK 包进行反编译。反编译后，生成的目录中的 AndroidManifest.xml 文件为 APK 包的配置文件，这个文件中包含了 APP 的配置信息，系统需要根据里面的内容运行 APP 的代码，显示界面。在配置文件 AndroidManifest.xml 中，uses-permission 标签中记录者 APP 安装时需要请求开启的权限信息。

我们使用 Python 进行编程，将输入文件夹内的 APK 文件全部读入，通过 APKtool 对所有 APK 包依次进行反编译，得到反编译完成后的生成文件。之后，程序对反编译生成目录中的配置文件 AndroidManifest.xml 进行解析，将含有 uses-permission 的行提取出来，输出到 newPmsnAlys.txt 文件中待处理。

之后对 newPmsnAlys.txt 文件中的文本进行处理。程序逐行读取该文件中的文本，将多余部分删除，只保留 APP 所请求的权限的名称信息。最终，将所有权限名称写入与 APK 包同名的文本文件中，放置在 result 文件夹中，等待后续的数据分析和处理。

5.2 推荐系统设计

在本软件中的应用的推荐系统，我们分为两个部分，分别为针对 APP 的权限推荐和针对社区用户的权限推荐。

5.2.1 针对 APP 的权限推荐系统

在针对 APP 的权限推荐中，我们没有采用比较经典但是相对准确率一般的传统方法，而是采用了近两年不论工业界还是学术界都非常流行的机遇深度学习的推荐系统模型。经过对多个模型的对比与研究，我们最终选择了在深度学习推荐系统领域相对比较经典的 DeepFM 模型。

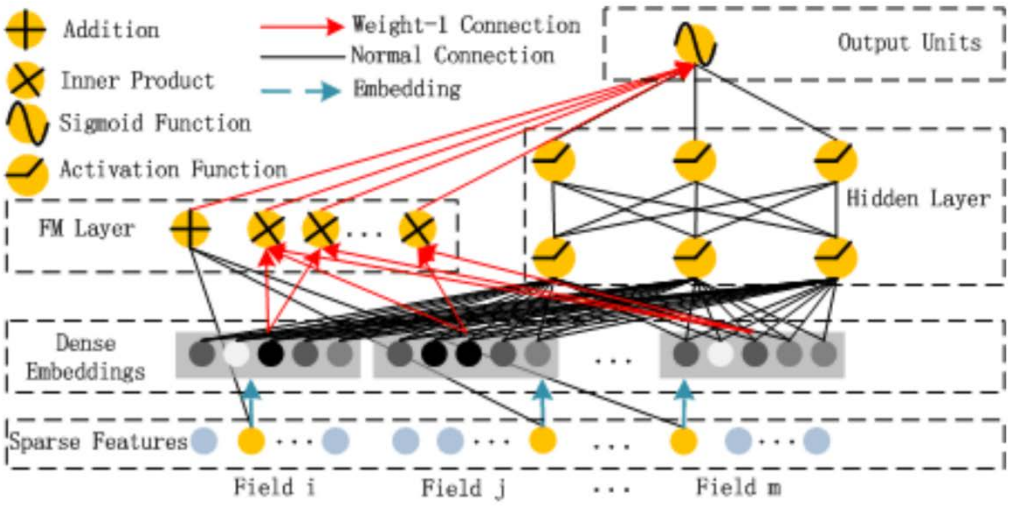

图 2 DeepFM 模型

DeepFM 出自华为诺亚方舟实验室 2017 年发表的论文《DeepFM: A Factorization-Machine based Neural Network for CTR Prediction》，模型结构如上图所示。DeepFM 是典型的网络融合结构之一——并行结构的典型代表。DeepFM 包含两部分：因子分解机部分和神经网络部分，分别负责低阶特征的提取和高阶特征的提取。

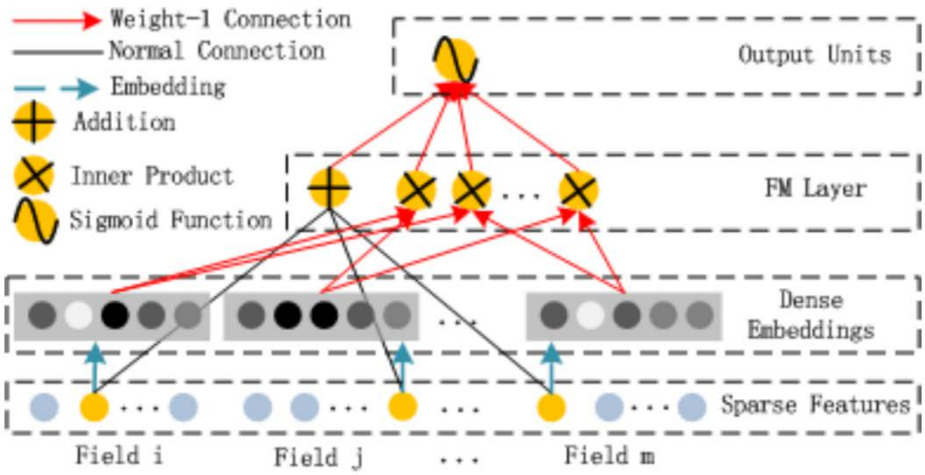

图 3 因子分解机部分

FM 部分是一个因子分解机，如上图所示。因为引入了隐变量的原因，对于几乎不出现或者很少出现的隐变量，FM 也可以很好的学习。

神经网络部分是一个前馈神经网络，如下图所示。

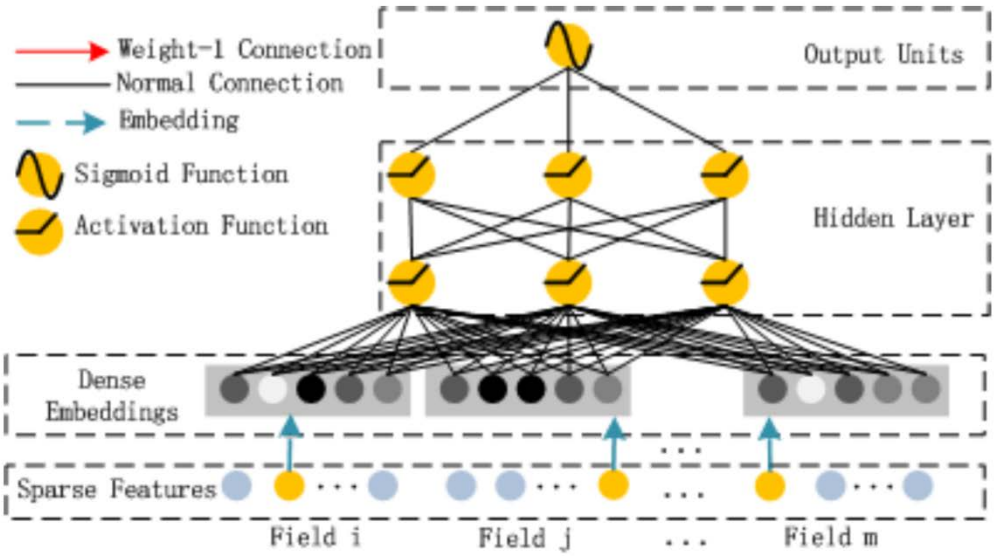

图 4 神经网络部分

与图像或者语音这类输入不同，图像语音的输入一般是连续而且密集的，然而在我们的权限推荐中，输入数据一般是及其稀疏的 onehot 向量，因此需要重新设计网络结构。具体实现中为，在第一层隐含层之前，引入一个嵌入层来完成将输入向量压缩到低维稠密向量。其结构如下图所示。

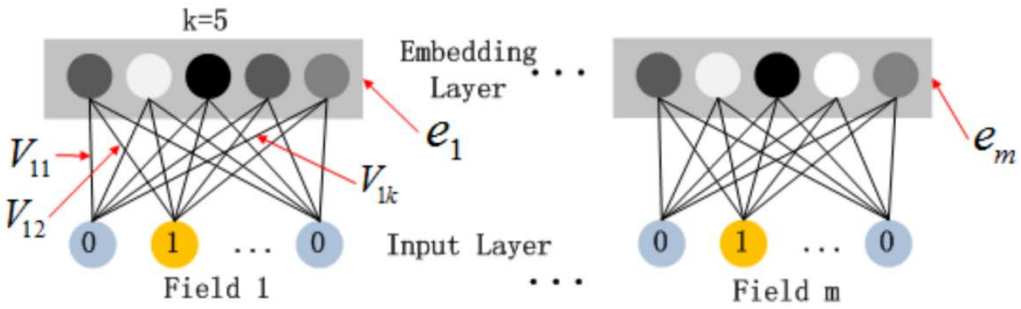

图 5 嵌入层结构

在嵌入层中，我们将所有的 onehot 向量“分而治之”，将特征分为不同的 field，便完成了高级特征的组合，减少了网络中的参数。

而在最终的输出层，与原本模型的 CTR 预估不同，我们将对软件权限的推荐看作一个多标签分类问题。输出层有多个函数为 Sigmoid 的节点组成，因此输出结果是一个维度等于权限总数、每个维度的值位于 0-1 之间的向量。我们将设置一个参数 x（0 < x < 1），输出量中对应位置的值大于 x 的维度所对应的权限

将被推荐。同时，我们将使用余弦相似度衡量输出向量与真是结果的相似度并将其作为损失函数，并在实验过程中调整 x 的数值使推荐的结果达到最好。

在软件中，我们将安卓 APP 权限解析工具中输出的结果中的每个权限转换为对应的 onehot 向量的表示形式，并将其作为特征输入到 DeepFM 模型中，得到输出的向量对应的权限即为向用户推荐的权限。

5.2.2 针对社区用户的权限推荐系统

在针对用户的权限推荐中，我们采用了相对比较传统的基于用户的协同过滤算法(user-based collaboratIve filtering)设计推荐系统。

基于用户的协同过滤算法是通过用户的历史行为数据发现用户对商品或内容的喜欢(如商品购买，收藏，内容评论或分享)，并对这些喜好进行度量和打分。根据不同用户对相同商品或内容的态度和偏好程度计算用户之间的关系。在有相同喜好的用户间进行商品推荐。

在我们的 APP 权限推荐系统中，如果 A，B 两个用户都测试了 x，y，z 三个 APP，则 A 和 B 属于同类用户，可以将 A 设置过的其他 APP 的权限推荐给 B。大体展示如下图所示。

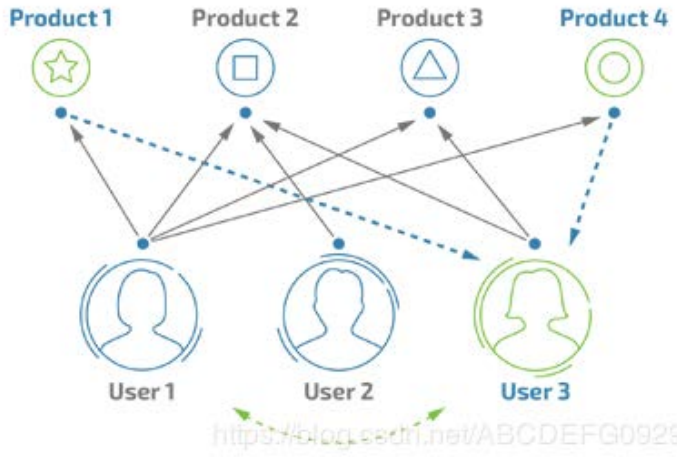

图 6 权限推荐

我们将用户解析权限或设置过权限的 APP 评分均置为 1，其他的 APP 评分置为 0，通过不同用户对于不同 APP 的喜好，寻找偏好相似的用户。我们通过皮尔逊相关度评价来计算并衡量用户之间的关系，其结果是一个介于-1 和 1 之间的值，该系数用来说明两个用户间联系的强弱程度。其分类为：

表 1 相关性评分

皮尔逊相关系数	数值
0.8-1.0	极强相关
0.6-0.8	强相关
0.4-0.6	中等程度相关
0.2-0.4	弱相关
0.0-0.2	极弱相关或无相关

该推荐无需过虑目标用户已有 APP，我们针对与目标用户相似的用户所解析过权限的 APP 进行评分与相似度的加权排序，最终为目标用户推荐最终评分较高的 APP 及其所开启的权限。

5.4 数据库详细设计

关系一：(apk) -[:require]-> (permission)

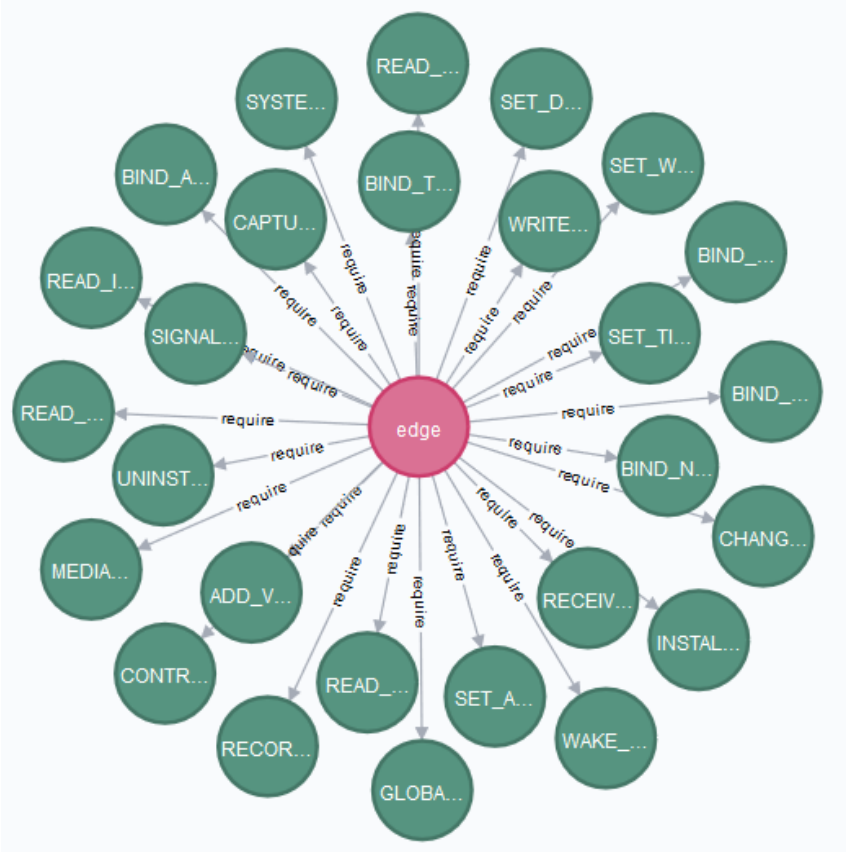

图 11 edge 浏览器所需要的全部权限

关系二：(user) -[:use]-> (apk) -[:allow]-> (permission)

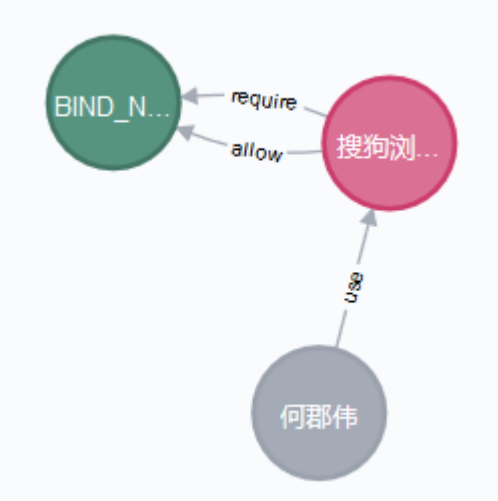

图 12 用户使用搜狗浏览器并且将其中某个需要的权限设置为允许

关系三：(user1) -[:friend]- (user2)

图 13 用户之间的好友关系

第六章 数据分析

6.1 数据集

我们将 APP 大致分为以下 5 类，Browser 类（浏览器软件）、Camera 类（照相软件）、Pay 类（支付软件）、Social 类（社交软件）以及 Video 类（视频软件），其中每个类型应用程序均收集了 10 个 APK，共 50 个进行权限分析。各 APP 信息以及其所需要的权限数量如图 11 所示。

	Browser	Camera	Pay	Social	Video
0	百度浏览器(37)	Faceu激萌(30)	钱站(35)	微博(41)	腾讯视频(36)
1	猎豹浏览器(36)	轻颜相机(24)	邮储银行(34)	百度贴吧(38)	优酷(33)
2	搜狗浏览器(36)	水印相机(24)	支付宝(34)	微信(36)	爱奇艺(32)
3	UC浏览器(29)	最美自拍(24)	兴业银行(31)	米聊(33)	西瓜视频(29)
4	edge(27)	b612(22)	360借条(31)	单身热恋(32)	咪咕视频(29)
5	chrome(26)	美妆相机(21)	小米贷款(30)	LOFTER(29)	芒果TV(28)
6	夸克(22)	无他相机(21)	滴滴金融(27)	闲聊(27)	央视影音(26)
7	360极速浏览器(17)	一甜相机(21)	闪银(26)	世纪佳缘(27)	bilibili(25)
8	久久浏览器(16)	美图秀秀(20)	云闪付(26)	最右(25)	抖音(23)
9	米侠浏览器(13)	最美证件照(9)	来分期(16)	一罐(23)	youtube(13)

图 7 APP 信息及其所需权限数量

6.2 权限数量及需求分析

将图 11 中的数据进行权限挖掘和分析，得到各 APP 所需要的权限信息以及权限数量。首先对 APP 所需权限数量进行分析，得到如下权限数量分布图。由图可知，应用程序所需权限数量在 25 项-35 项之间的所占比例最多，高达 70%，而在此之中需要 25 项权限信息的应用程序又达到了 30%；APP 所需权限数量在 15 项以下或 35 项以上的比例较少，分别为 12%和 6%。

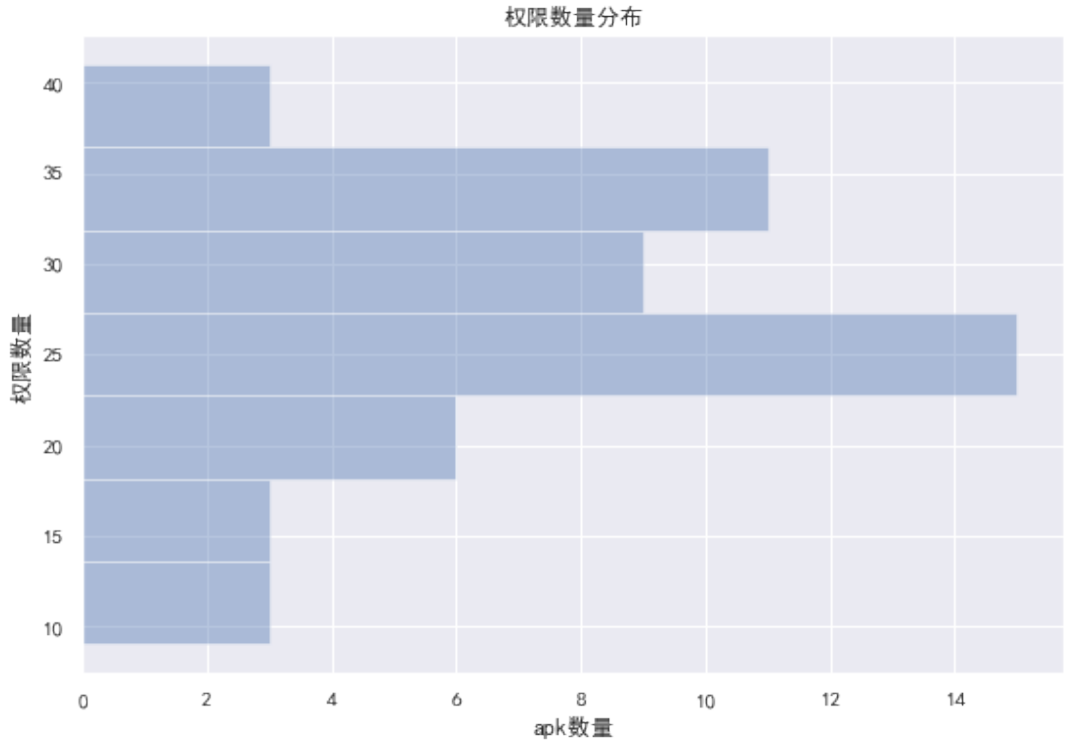

图 8 权限数量分布

与此同时，对 APP 所需权限信息进行分析，根据各权限在 50APK 中的需求次数进行排序，得到如图 13 所示。由图可知，以下 5 项权限所需次数最多，在统计的 50 个数据中，每个 APK 均需要，分别为：SET_ALWAYS_FINISH（允许程序设置程序在后台是否总是退出）、READ_SMS（允许程序读取短信内容）、BIND_TELECOM_CONNECTION_SERVICE（必须由 ConnectionService 要求，确保只有系统可以绑定到它）、CHANGE_WIFI_MULTICAST_STATE（允许程序改变 WiFi 多播状态）以及 BLUETOOTH_PRIVILEGED（允许应用程序配对蓝牙设备，而无需用户交互。这不是第三方应用程序可用）。其次，需求最多的 10 项权限信息如图 14 所示。

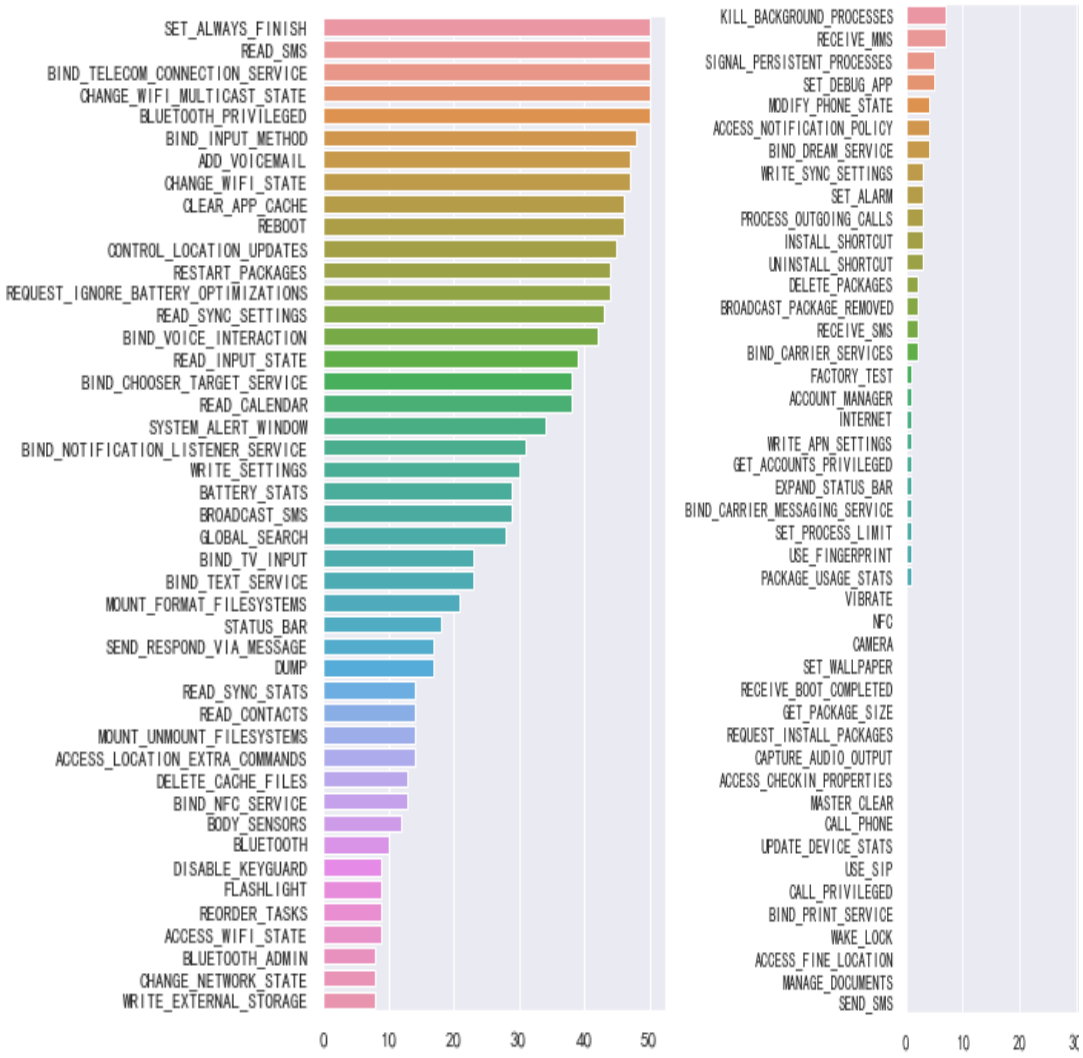

图 9 权限需求次数

	description	num
SET_ALWAYS_FINISH	允许程序设置程序在后台是否总是退出	50
READ_SMS	允许程序读取短信内容	50
BIND_TELECOM_CONNECTION_SERVICE	必须由ConnectionService要求，确保只有系统可以绑定到它	50
CHANGE_WIFI_MULTICAST_STATE	允许程序改变WiFi多播状态	50
BLUETOOTH_PRIVILEGED	允许应用程序配对蓝牙设备，而无需用户交互。这不是第三方应用程序可用	50
BIND_INPUT_METHOD	请求InputMethodService服务，只有系统才能使用	48
ADD_VOICEMAIL	允许一个应用程序添加语音邮件系统	47
CHANGE_WIFI_STATE	允许程序改变WiFi状态	47
CLEAR_APP_CACHE	允许程序清除应用缓存	46
REBOOT	允许程序重新启动设备	46

图 10 需求最多权限 top10

6.3 各类型数据分析

我们针对以上 5 个分类，分别对各类型的 APP 进行了权限分析，得到各类型需求最多的 10 项权限信息。Browser 类需求最多的权限信息如图 15 所示，由图可以看出，Browser 类需求最多的权限信息为 RECEIVE_BOOT_COMPLETED，即允许程序开机自动运行。

	description	num
RECEIVE_BOOT_COMPLETED	允许程序开机自动运行	10
DIAGNOSTIC	允许程序到RW到诊断资源	10
BIND_NFC_SERVICE	由HostApduService或OffHostApduService必须确保只有系统可以绑定到它	10
BIND_TELECOM_CONNECTION_SERVICE	必须由ConnectionService要求，确保只有系统可以绑定到它	10
WRITE_VOICEMAIL	允许应用程序修改和删除系统中的现有的语音邮件，只有系统才能使用	10
ACCESS_LOCATION_EXTRA_COMMANDS	允许应用程序访问额外的位置提供命令	10
BROADCAST_WAP_PUSH	WAP PUSH服务收到后触发一个广播	10
CAPTURE_SECURE_VIDEO_OUTPUT	允许一个应用程序捕获视频输出。不被第三方应用使用	10
BIND_CARRIER_SERVICES	允许绑定到运营商应用程序中的服务的系统进程将有这个权限	9
INSTALL_SHORTCUT	创建快捷方式	9

图 11 Browser 类需求最多权限 top10

Camera 类需求最多的权限信息如图 16 所示，由图看以看出，Camera 类需求最多的权限信息为 GET_TASKS，即允许一个程序获取信息有关当前或最近运行的任务，一个缩略的任务状态，是否活动等等。

	description	num
GET_TASKS	允许一个程序获取信息有关当前或最近运行的任务，一个缩略的任务状态，是否活动等等	10
BODY_SENSORS	允许应用程序访问用户使用的传感器来测量他/她的身体内发生了什么，如心率仪	10
DIAGNOSTIC	允许程序到RW到诊断资源	10
READ_SYNC_SETTINGS	允许程序读取同步设置，读取Google在线同步设置	10
BIND_TV_INPUT	必须由TvInputService需要确保只有系统可以绑定到它	10
READ_CALENDAR	允许程序读取用户的日程信息	10
UNINSTALL_SHORTCUT	删除快捷方式	9
BROADCAST_PACKAGE_REMOVED	允许程序广播一个提示消息在一个应用程序包已经移除后	9
MOUNT_FORMAT_FILESYSTEMS	允许程序格式化可移动文件系统，比如格式化清空SD卡	9
BIND_VPN_SERVICE	绑定VPN服务必须通过VpnService服务来请求,只有系统才能用	9

图 12 Camera 类需求最多权限 top10

Pay 类需求最多的权限信息如图 17 所示，由图看以看出，Pay 类需求最多的权限信息为 GET_TASKS，即允许一个程序获取信息有关当前或最近运行的任务，一个缩略的任务状态，是否活动等等。

	description	num
GET_TASKS	允许一个程序获取信息有关当前或最近运行的任务，一个缩略的任务状态，是否活动等等	10
BIND_VPN_SERVICE	绑定VPN服务必须通过VpnService服务来请求,只有系统才能用	10
ACCESS_LOCATION_EXTRA_COMMANDS	允许应用程序访问额外的位置提供命令	10
DIAGNOSTIC	允许程序到RW到诊断资源	10
READ_SYNC_SETTINGS	允许程序读取同步设置，读取Google在线同步设置	10
BIND_TV_INPUT	必须由TvInputService需要确保只有系统可以绑定到它	10
READ_CALENDAR	允许程序读取用户的日程信息	10
BIND_WALLPAPER	必须通过WallpaperService服务来请求，只有系统才能用	10
RECEIVE_BOOT_COMPLETED	允许程序开机自动运行	10
BODY_SENSORS	允许应用程序访问用户使用的传感器来测量他/她的身体内发生了什么，如心率仪	10

图 13 Pay 类需求最多权限 top10

Social 类需求最多的权限信息如图 18 所示，由图看以看出，Social 类需求最多的权限信息为 GET_TASKS，即允许一个程序获取信息有关当前或最近运行的任务，一个缩略的任务状态，是否活动等等。

	description	num
GET_TASKS	允许一个程序获取信息有关当前或最近运行的任务，一个缩略的任务状态，是否活动等等	10
BROADCAST_PACKAGE_REMOVED	允许程序广播一个提示消息在一个应用程序包已经移除后	10
READ_CALENDAR	允许程序读取用户的日程信息	10
ACCESS_LOCATION_EXTRA_COMMANDS	允许应用程序访问额外的位置提供命令	10
MODIFY_AUDIO_SETTINGS	允许程序修改声音设置信息	10
READ_SYNC_SETTINGS	允许程序读取同步设置，读取Google在线同步设置	10
BIND_TV_INPUT	必须由TvInputService需要确保只有系统可以绑定到它	10
BIND_VPN_SERVICE	绑定VPN服务必须通过VpnService服务来请求,只有系统才能用	10
UNINSTALL_SHORTCUT	删除快捷方式	10
BODY_SENSORS	允许应用程序访问用户使用的传感器来测量他/她的身体内发生了什么，如心率仪	10

图 14 Social 类需求最多权限 top10

Video 类需求最多的权限信息如图 19 所示，由图看以看出，Video 类需求最多的权限信息为 GET_TASKS，即允许一个程序获取信息有关当前或最近运行的任务，一个缩略的任务状态，是否活动等等。

	description	num
GET_TASKS	允许一个程序获取信息有关当前或最近运行的任务，一个缩略的任务状态，是否活动等等	10
READ_SYNC_SETTINGS	允许程序读取同步设置，读取Google在线同步设置	10
DIAGNOSTIC	允许程序到RW到诊断资源	10
BODY_SENSORS	允许应用程序访问用户使用的传感器来测量他/她的身体内发生了什么，如心率仪	10
BIND_TV_INPUT	必须由TvInputService需要确保只有系统可以绑定到它	10
BIND_VPN_SERVICE	绑定VPN服务必须通过VpnService服务来请求,只有系统才能用	10
MODIFY_AUDIO_SETTINGS	允许程序修改声音设置信息	9
ACCESS_LOCATION_EXTRA_COMMANDS	允许应用程序访问额外的位置提供命令	9
READ_CALENDAR	允许程序读取用户的日程信息	9
RECORD_AUDIO	允许程序录制声音通过手机或耳机的麦克	9

图 15 Video 类需求最多权限 top10

以上分析可知，除 Browser 类需求最多的权限信息为允许程序开机自动运行外，其余各类需求最多的权限信息均为允许一个程序获取信息有关当前或最近运行的任务，一个缩略的任务状态，是否活动等等。

第七章 测试分析

7.1. 权限提取功能测试

权限提取功能是本系统中最基本的功能，在该功能实现之后，后续所有的功能测试都需要依赖从 APK 中提取的权限数据文件。我们的测试目标是：能够正确的逆向编译 APK，并成功提取其中的权限信息。我们选取了 50 个 APK 文件，最终的测试结果是，我们的工具可以在有限的时间范围内得到这些 APK 文件的权限信息。

7.2. 数据库存取功能测试

对于数据库功能的测试，我们的测试计划如下表：

项目名称:	APK 权限分析工具		配置版本:	Windows10	
测试人:			测试时间:	2019.11.20	
用例编号: 01					
用例目的: 测试插入、修改基本功能					
前提条件: neo4j 数据库启动服务					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0101					
用例编号: 02					
用例目的: 测试查询、删除基本功能					
前提条件: neo4j 数据库启动服务					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0201					
用例编号: 03					
用例目的: 测试数据库查询和插入的性能					
前提条件: neo4j 数据库启动服务					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0301					

7.3. 社区功能测试

对于社区功能的测试，我们的测试计划如下表：

项目名称:	APK 权限分析工具		配置版本:	Windows10	
测试人:			测试时间:	2019.11.25	
用例编号: 01					
用例目的: 测试登陆功能					

前提条件：无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0101					
用例编号：02					
用例目的：测试退出功能					
前提条件：无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0201					
用例编号：03					
用例目的：测试用户注册功能					
前提条件：无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0301					
用例编号：04					
用例目的：测试用户添加好友功能					
前提条件：无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0401					
用例编号：05					
用例目的：测试用户基本信息展示功能					
前提条件：无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0501					
用例编号：06					
用例目的：测试用户发帖功能					
前提条件：无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0601					
用例编号：07					
用例目的：测试用户收藏帖子功能					
前提条件：无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0701					
用例编号：08					
用例目的：测试用户好友管理功能					
前提条件：无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0801					

7.4. 推荐功能测试

对于推荐功能的测试，我们的测试计划如下表：

项目名称:	APK 权限分析工具	配置版本:	Windows10
测试人:		测试时间:	2019.11.25

用例编号: 01					
用例目的: 测试权限收集功能					
前提条件: 无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0101					
用例编号: 02					
用例目的: 测试权限挖掘及分析功能					
前提条件: 无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0201					
用例编号: 03					
用例目的: 测试权限推荐功能					
前提条件: 无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0301					
用例编号: 04					
用例目的: 测试权限设置功能					
前提条件: 无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0401					
用例编号: 05					
用例目的: 测试一键应用权限功能					
前提条件: 无					
子用例编号	输入	操作步骤	期望结果	实测结果	备注
0501					