**2018年全国大学生信息安全竞赛**

**作品报告**

**作品名称：移动互联网中基于用户行为的隐私保护机制及应用**

**电子邮箱：**

**提交日期：**

填写说明

1. 所有参赛项目必须为一个基本完整的设计。作品报告书旨在能够清晰准确地阐述（或图示）该参赛队的参赛项目（或方案）。

2. 作品报告采用A4纸撰写。除标题外，所有内容必需为宋体、小四号字、1.5倍行距。

3. 作品报告中各项目说明文字部分仅供参考，作品报告书撰写完毕后，请删除所有说明文字。(本页不删除)

4. 作品报告模板里已经列的内容仅供参考，作者可以在此基础上增加内容或对文档结构进行微调。

5. 为保证网评的公平、公正，作品报告中应避免出现作者所在学校、院系和指导教师等泄露身份的信息。

**目 录**

[摘要 1](#_Toc514873497)

[第一章 作品概述 2](#_Toc514873498)

[1.1 背景 2](#_Toc514873499)

[1.2 相关概念 2](#_Toc514873500)

[1.3 特色描述 3](#_Toc514873501)

[1.4 应用前景分析 4](#_Toc514873502)

[第二章 作品设计与实现 5](#_Toc514873503)

[2.1 模型表示 5](#_Toc514873504)

[2.2 信任值计算 6](#_Toc514873505)

[2.3 应用设计 14](#_Toc514873506)

[第三章 作品测试与分析 15](#_Toc514873507)

[3.1 测试方案 15](#_Toc514873508)

[3.2 测试数据 16](#_Toc514873509)

[第四章 创新性说明 27](#_Toc514873510)

[4.1 现状简述 27](#_Toc514873511)

[4.2 创新性综述 29](#_Toc514873512)

[第五章 总结 30](#_Toc514873513)

[参考文献 32](#_Toc514873514)

# 摘要

移动互联网技术正在发展，社交网络逐渐成为人们日常生活重要的一部分。用户在各类社交网络平台上公开个人信息和分享实时动态的同时，也带来了隐私泄露的风险。用户需要一种隐私保护机制，来更加有效地保护用户在移动社交平台上的个人信息不被滥用。

本作品针对了当前的隐私保护方法不能很好保护移动互联网中用户隐私数据的问题，结合移动互联网环境下用户行为的特点，提出了移动互联网中基于用户行为的隐私保护机制及其应用。在研究过程中，首先通过系统有效的对移动互联网环境下用户行为的分析与特征提取，构建访问控制模型；之后，通过爬虫技术获取构建访问控制模型所需要的数据集并对数据进行预处理与特征提取工作，将爬取后的信息存储在MongoDB数据库中；在完成数据获取工作后，将数据进行模型训练，通过对用户个人信息与用户行为信息进行分析获取用户信任值实现由用户操作到访问权限的映射，实现访问控制模型系统；最终，将该隐私保护系统部署于由本小组独立设计的安卓仿移动社交APP服务端，模拟隐私保护。

整个模型展现出良好的应用价值，能够提高当前社交网络的服务质量，同时也为后续的隐私保护机制研究提供了新思路。

# 第一章 作品概述

1.1 背景

近年来随着移动互联网技术的不断发展，社交网络的用户数量呈现了持续增长的趋势。国内的微博、贴吧、豆瓣等社交网络平台都具有十分庞大的规模。2017年Q3微博财报数据显示，截至2017年9月，微博月活跃用户达到了3.76亿。用户在各大社交平台发布的各种形式的内容不计其数，与此同时，社交网络的用户之间也会发生大量的交互行为。

社交网络在改变人们生活方式的同时，也面临着保护用户隐私安全的问题。用户在注册社交网络账户的时候，往往需要提供个人资料，其中包括姓名、电话、家庭住址、电子邮件等敏感信息。与此同时，用户在社交网络平台上分享的各种文字、图片和地理位置等也包含大量的个人隐私。一旦这些信息发生泄漏，用户可能会面临短信、电话和垃圾邮件的骚扰，甚至可能会遭遇欺诈、身份冒用和网络钓鱼等危险。尽管当前的社交网络中都提供与隐私相关的设置，但由于用户普遍缺乏安全意识，且隐私设置通常较为繁琐，因而大部分用户都选择了默认的隐私设置。社交网络作为人际交往和信息共享的平台，其默认的隐私设置具有很大程度的开放性，并不能满足用户的隐私保护需求。因此如何在社交网络系统中构建有效的隐私保护机制，成为了学者们关注的热点问题。

1.2 相关概念

1.2.1 社交网络

社交网络(SNS， Social Network Service)作为以互联网技术为基础的社交服务平台，提供了内容分享、交友互动、信息传播、搜索和推荐等功能，具有开放性、实时性、娱乐性和互动性等特点。当前的社交网络主要以社交网络网站(Social Network Site)的形式呈现，例如博客、内容社区、个人空间、交友平台、论坛和微博等。社交网络的核心是用户、关系和内容。

用户：社交网络的用户可以是真实的个人，也可以是虚拟的角色。用户是社交网络的独立行为个体，用户的数量代表了的规模，社交网络的发展受到用户数量变化和用户活跃程度的影响。

关系：社交网络中的关系指用户与用户之间产生联系的方式。在实际的人际交往中存在着朋友、同学和同事等多种关系，这些关系映射到虚拟的社交网络中，统一表现为关注和好友的形式。

内容：社交网络中的内容可以有多种形式，可以是简单的文本信息，也可以是图片、网址链接、音频和视频等多媒体信息。这些内容可以由用户原创发布产生，也可以来自用户的评论和转发等行为。

对于社交网络的研究围绕用户、关系和内容这三个要素展开，总体上可以分为社交网络结构研究和社交网络用户行为的研究者两类。其中社交网络结构的研究主要关注用户和关系。为了建立社交网络结构的数学模型，通常将用户抽象为节点，用户之间的关系抽象为边，那么就得到了社交网络的图模型来。对于社交网络结构的分析，通常要借鉴图论和复杂网络等领域的研究。社交网络用户行为的研究主要关注内容这一块，即通过分析用户发布的信息特征来得到用户行为的一些规律。

1.2.2 隐私保护

在信息膨胀和大数据的时代，用户的个人隐私安全是信息安全的一个重要的方面。云计算、电子商务和社交网络等当下流行的互联网应用中都包含大量用户隐私数据。隐私保护是访问控制系统不可或缺的功能，相关的基本概念如下：

访问控制系统：一般来说，访问控制模型由主体、客体和控制策略三部分组成。其中主体是发起访问控制请求的一方，客体是主体请求访问的资源对象，控制策略规定了主体对客体进行访问时需要满足的条件。

隐私信息：社交网络中广泛存在用户的敏感信息，例如姓名、居住地、学校、生日、手机号码和电子邮箱等个人资料。另外用户分享的文字、图片、音频、视频、地理位置和设备名称也分别不同程度地包含一些敏感的信息。

1.3 特色描述

本作品针对现有隐私保护方法在移动互联网环境下隐私保护力不足以及数据失真的问题，给出了移动互联网环境下基于用户行为的隐私保护机制。通过对用户身份与用户行为的判别，为不同的用户提供不同的访问服务，高信任值用户的合法行为可以获得高保真的数据，而低信任值用户或高信任值用户的非法行为则只能获取失真的数据甚至被拒绝服务，从而在保护隐私数据的同时提高服务质量和用户体验。

通过研究移动互联网环境下基于用户行为的访问控制模型的相关定义，我们提出了移动互联网环境下基于用户信任值的访问控制模型，给出基于PageRank用户关系、

K-means时间聚类、遗忘曲线的信任值计算方法，并通过仿真实验验证了模型的有效性。

1.4 应用前景分析

社交网络作为当前流行的信息分享和人际交往的平台，包含了大量用户个人信息和隐私数据，由于社交网络开放共享的特性，用户的隐私数据往往处于不安全的状态，因此研究社交网络中的隐私保护机制具有重要的意义。

当下社交网络的基本设置有很大的相似性，尤其是个人信息模块、内容发布模块、交友模块，基本在每个社交平台都能找到。我们提出的基于用户行为的社交网络隐私保护机制，主要建立在上述基本的社交网络功能上，基于用户的基本信息和用户的行为信息，可以普遍覆盖当下流行的移动互联网社交平台，例如微博、贴吧、豆瓣等，因而具有广泛的应用前景。

# 第二章 作品设计与实现

2.1 模型表示

研究移动互联网环境下的用户行为特点以及访问控制特性，构建访问控制模型。

移动网络环境中的用户行为信息主要包括移动网络环境下的用户信息和移动网络环境下的行为信息。其中，用户信息是对用户静态属性的表述，行为信息则是对用户的一系列动态操作的表述。而用户信息又包括了用户的个人资料信息和用户之间的好友关系。

用户的个人信息主要包括用户的一些基本信息，例如姓名、性别、出生日期、昵称、所在地、个人简介等。 用户的每个属性信息都可以看成是二维平面的一个点，纵轴是不可变的属性，包括出生日期、姓名、性别等。横轴是可变的用户属性，包括所在地、年龄、昵称、关注用户数、被关注用户数、是否认证等。 因为当前所在地会随着用户居住地的变化而变化，年龄会随着时间变化，关注用户数与被关注用户数则是基于用户的操作动态变化的。

好友关系是一个巨大的带权有向图，用户之间的好友关系显然也是考虑用户是否值得信任的一个重要考虑环节。

用户行为信息指用户一系列操作的集合，包含了时间，地点，内容等维度，我们希望模型能够对用户行为进行及时的反馈从而更新用户信任值。

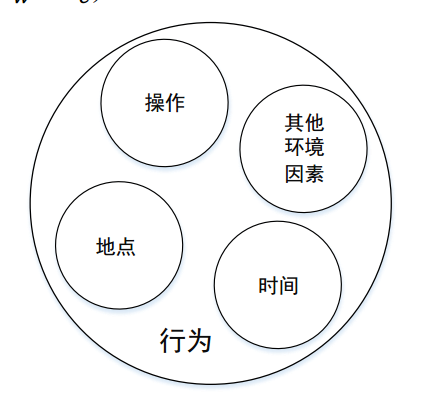


图2.1 行为的基本构成

在构建的模型中，我们希望能通过模型分析用户信息和用户行为信息得到用户信任值，进行访问等级到隐私需求的映射，进而进行对原始数据的限制发布，最终用户获取到的是限制发布处理后的数据。

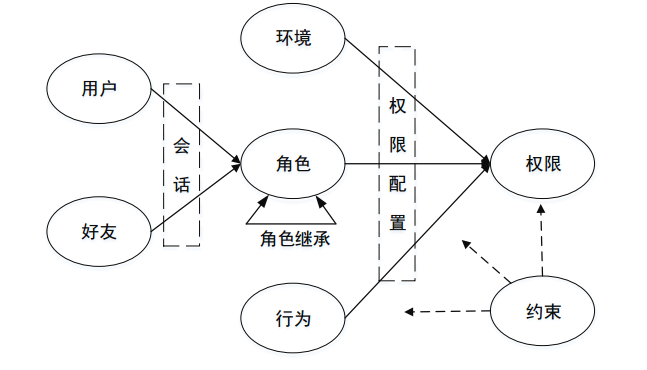


图2.2 访问控制模型基本结构

2.2 信任值计算

2.2.1 计算运用算法介绍

1. **PageRank**

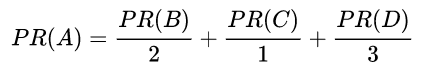
PageRank是一种由根据网页之间相互的超链接计算的技术。Google用它来体现网页的相关性和重要性，在搜索引擎优化操作中是经常被用来评估网页优化的成效因素之一。

PageRank通过网络浩瀚的超链接关系来确定一个页面的等级。Google把从A页面到B页面的链接解释为A页面给B页面投票，Google根据投票来源（甚至来源的来源，即链接到A页面的页面）和投票目标的等级来决定新的等级。简单的说，一个高等级的页面可以使其他低等级页面的等级提升。

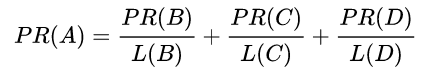
假设一个由4个网页组成的群体：A，B，C和D。如果所有页面都只链接至A，那么A的PR（PageRank）值将是B，C及D的PageRank总和。



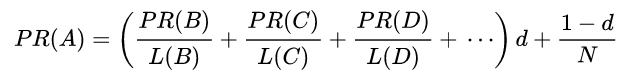
重新假设B链接到A和C，C只链接到A，并且D链接到全部其他的3个页面。一个页面总共只有一票。所以B给A和C每个页面半票。以同样的逻辑，D投出的票只有三分之一算到了A的PageRank上。



换句话说，根据连出总数平分一个页面的PR值。



最后，所有这些被换算为一个百分比再乘上一个系数d。由于没有向外链接的网页传递出去的PageRank会是0，所以通过数学系统给了每个页面一个最小值

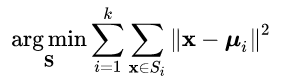


要注意在Sergey Brin和Lawrence Page的1998年原文中给每一个页面设定的最小值是 1-d，而不是这里的 (1-d)/N。 所以一个页面的PageRank是由其他页面的PageRank计算得到。不断的重复计算可以得到所有网页的PageRank。如果给每个网页一个随机PageRank值（非0），那么经过不断的重复计算，这些页面的PR值会趋向于稳定，也就是收敛的状态。这就是搜索引擎使用它的原因。

1. **K-means**

k-平均算法源于信号处理中的一种向量量化方法，现在则更多地作为一种聚类分析方法流行于数据挖掘领域。k-平均聚类的目的是：把 n个点（可以是样本的一次观察或一个实例）划分到k个聚类中，使得每个点都属于离他最近的均值（此即聚类中心）对应的聚类，以之作为聚类的标准。这个问题将归结为一个把数据空间划分为Voronoi cells的问题。

已知观测集 ()，其中每个观测都是一个d-维实向量，k-平均聚类要把这n个观测划分到k个集合中(k≤n)，使得组内平方和（WCSS within-cluster sum of squares）最小。换句话说，它的目标是找到使得下式满足的聚类，



其中是 中所有点的均值。

1. **最优分割法**

最优分割法是1958年由Fisher提出的一种处理有序资料的分类方法，用于寻找线性有序数据集的最优分割点。基本思想是现将n个样品看成一类，然后依据分类的误差函数逐渐增加分类。

设有序样品一次为X(1)，X(2)，…，X(n)(X(i)为m维向量).

用b(n，k)表示将n个有序样品分为k类每一类为

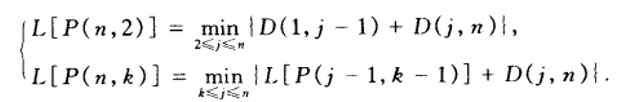
设某一类G包含的样品有()，记为G={i，i+1，i+2，…，j}，则该类的均值向量

用D(i ， j)表示这一类的直径，常用的直径有：

定义这种分类法的损失函数为

当n、k固定时，L[b(n，k)]越小表示各类的离差平方和越小，分类是合理的。因此要寻找一种分法b(n，k)，使分类损失函数L达最小。记P(n，k)是使损失函数达到极小的分类法。

该分类法最核心的部分是利用以下两个递推公式:



上面由定义就可证明如果要找将n个样品分为k类的最优分割，应建立在将j-1个样品分为k-1类的最优分割基础上。

总之，为了求最优解，主要是计算和

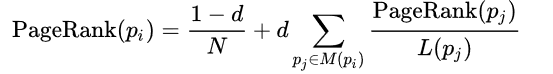
2.2.2 计算过程介绍

1. **计算过程概述**

通过对用户行为信息与个人信息进行分析获取用户信任值实现由用户操作到访问权限的映射用户的初始信任值主要是从已经采集的用户信息中评定用户的初始信任值，对用户信息中的每个属性e设置不同权重q，之后进行归一化处理，最终得到用户初始信任值。

****

有些用户可能因为基础信息填写不准确而导致用户初始信任值结果不准确，因此我们使用PageRank算法对用户关系网进行处理，对用户初始信任值进行处理。



用户的信任值更新包括了时间驱动与事件驱动两部分。用户的信任值遗忘则采用了符合艾宾浩斯的遗忘曲线，即遗忘的速度是不均匀的，起初遗忘的速度最快，然后会逐渐变慢，慢慢地趋于一个稳定值。因此每个行为信任值将依据遗忘曲线进行更新。

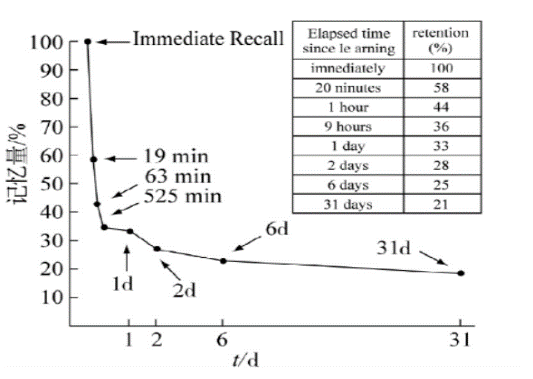


图2.3 艾宾浩斯遗忘曲线

用户每次操作，包括发布信息，浏览信息，登录等均具有时间、位置、操作、内容等属性，而模型通过时间聚类、位置聚类、文本分词等手段对用户操作进行分析，用户每一次的操作行为都会有一个反馈，良好的操作行为会形成正反馈，而不安全的行为则会形成负反馈。用户每次行为对信任值的影响与时间反馈均会对用户总信任值产生影响，最终通过后台访问控制配置得到访问控制模型。

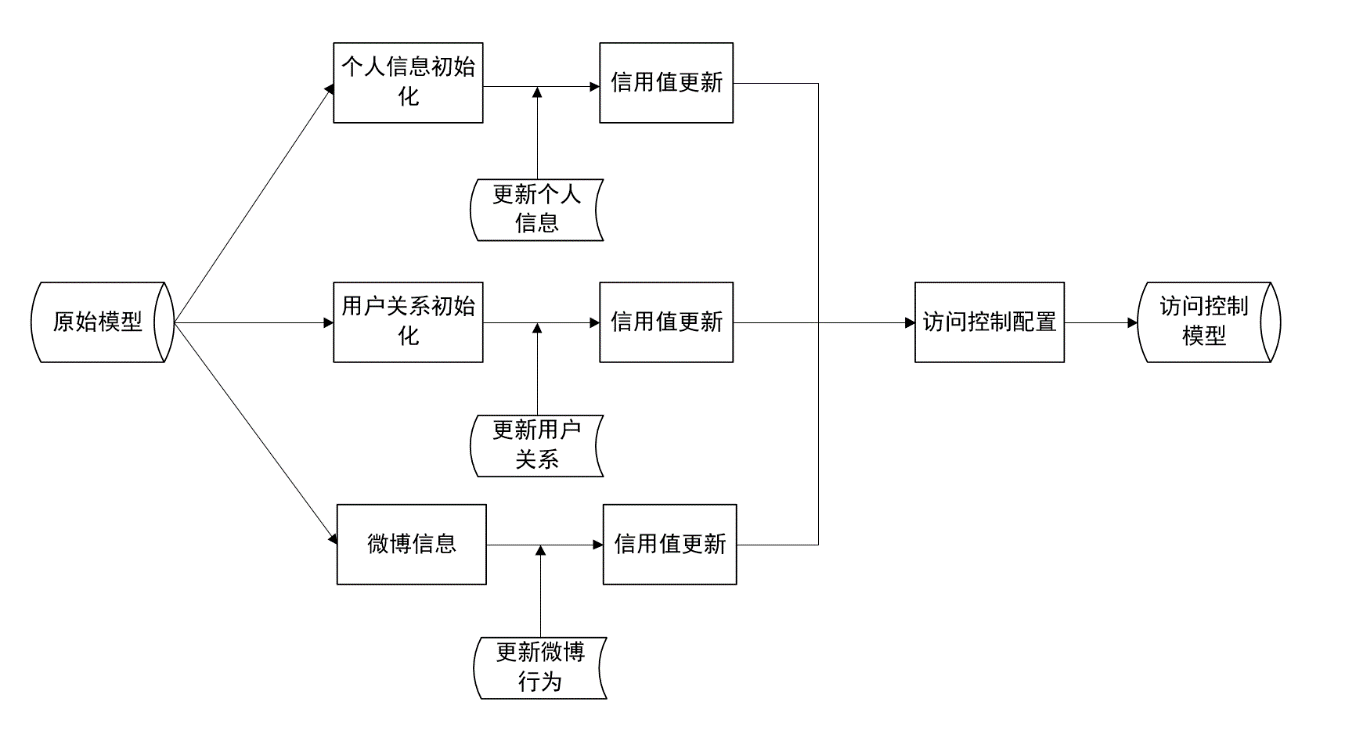


图2.4 模型构建流程

1. **时间聚类**

时间聚类的流程图如下所示：



图2.5 时间聚类流程图

首先，我们将每个用户各自的微博发布时间汇总，对每个用户的微博时间数据使用K-means算法进行聚类，这里我们对于聚类类别分别用3、4、5类进行了实验，最终发现聚类类别数为3的时候聚类效果最好，同时也最符合人们的日常APP使用习惯。每个人的日常使用微博时间无非三个时间点，午休时间，晚饭后的一段时间，以及睡觉前的一段时间，可能每个人的时间略有偏差，但是大致的时间段差不多是分布在三个区间中。故我们将每个用户的微博时间数据进行聚类，就能够得到每个用户的三个发布微博的时间中心。

之后将用户的所有微博数据与三个时间中心计算差异值，这里我们的差异值D采用的计算公式如下所示，假设三个中心点的坐标分别为

这里采用倒数相加求和的方式是因为我们需要保证当一个用户的某次微博发布行为严重偏离三个中心位置时，所得出的差异值会异常的大，而分母的分母中的0.01是为了防止某个点与聚类中心想重合导致的除零问题。

计算完每个用户的差异值的集合之后，我们将所有用户的所有差异值汇总。由于一天中只有24个小时，而我们的数据也是计算过差异的数据，已经将一天中发布时间的特征消除，所以剩下的数据具有一个共性，那就是当用户的某次行为接近自身的三个中心点时，得出的D会较小，反之较大。并且由于一天的时间跨度固定，所以此D一定是一个有上限的值。

我们对于D的集合进行一个二分，就可以得出用户异常行为的异常值的阈值。当用户的行为的异常值超过这个阈值，就能够认为用户的行为是具有一定危险性的。

对于所有用户的所有差异值进行分类显然时间和空间代价太高。而且若用一个过于准确的差异值去定义阈值也没有太高的必要性，故我们对于D的集合首先进行归一化处理。之后对于D’∈[0，1]的这些数据进行分类，将[0，1]的区间分100类，统计在每个区间中的异常值的数量，这样就得出了一个异常值的数量变化曲线。此时就能够通过对于这个曲线分段的方法来得到合理阈值。

对于这样的一个变化曲线来说，由于只能将曲线二分，故我们选择采用有序聚类的方法，对于上述的一百个区间的数据进行有序聚类，确定一个曲线的最优分割，这个最优分割的区间下标代表的是区间中的数量变化最快的一个点。显然合法行为和危险行为的数量上存在着绝对的差别，故我们通过寻找区间中数量急剧变化的点的方法是合理的。

通过上述方法，我们能够得出一个系统的合法行为的差异值阈值。这样每个用户在进行某个行为时，通过将系统时间与用户个人的三个中心点计算本次操作的差异，如果差异达到阈值，则进行验证。

1. **用户关系网络分析**

用户之间存在着关注与被关注的关系，每个用户的“可信度”与他的被关注者与关注者数量密不可分，而用户关注另一个用户在图上可以看成一条有向边，而网页与超链接到另一个网页与该结构类似，因此网页排名算法与用户信任值算法具有共性。因此我们使用了Google的PageRank算法对用户组成的关系网络进行处理，使每个用户获得一个用户关系权重带来的收益值，对用户总体信任值进行更新。

1. **登陆设备验证**

在移动互联网中用户的时间或位置都在不断移动当中，但移动终端设备一般不会轻易变动，所以我们将用户登录常用设备进行存储，并在用户每次登录时进行验证，若用户使用非常用设备登录，可以很大程度怀疑用户遭遇了盗号或撞库，后台强制进行短信验证以保证用户登陆的安全性，只有当用户验证通过才准允登录并将新设备存储为常用设备。

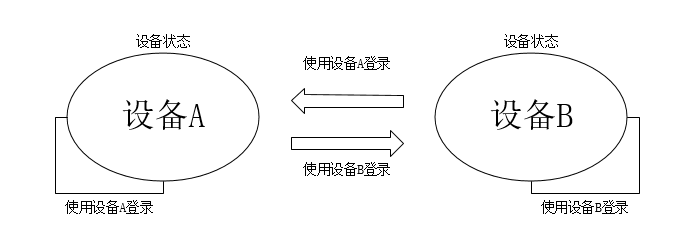


图2.6 常用设备状态转换

1. **信任值更新**

用户信任值在每次用户进行操作与时间节点进行更新，用户进行操作时将每次信任值更新状态写入数据库修改用户信任值，而在每小时对用户的操作信任值进行遗忘公式处理，使用户每次操作造成的影响随时间推移减小。因为每天凌晨用户活跃度较小，故2:00数据端将进行用户信任值的重新计算，具体操作包括更新时间聚类中心点，更新用户关系网权值，汇总微博转评赞等，最终实现模型信任值的更新处理。

2.3 应用设计

将基于行为的访问控制模型的隐私保护系统部署在模拟社交APP中，通过应用效果来展示隐私保护机制的有效性和准确性。

该APP模拟实现了新浪微博的登录，查看微博，查看用户信息等功能。隐私保护系统主要分为两部分，一部分是手机客户端，主要是与用户进行交互，获取用户相关的信息，并将对应的信息展现给用户。另一部分则是服务端，部署隐私保护系统，包括用户行为分析、限制发布的实现等。

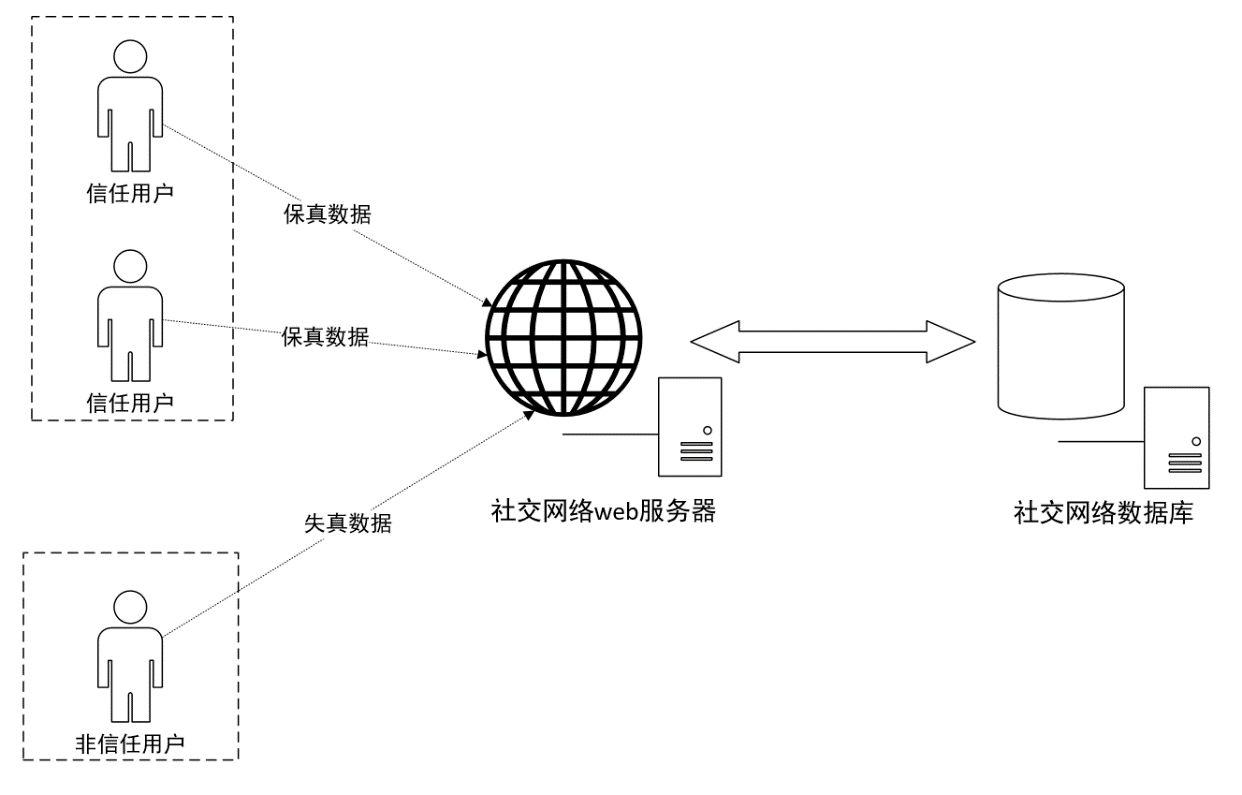


图2.7 隐私保护系统

隐私保护系统的隐私保护模块部署于服务端。该套隐私保护系统包含三部分，分别是 Web 服务器、计算机群和数据库服务器。其中，Web 服务器主要负责用户操作行为获取，并进行简单的行为特征提取，另外作为与客户端唯一交互的服务器，同时具备有访问控制的功能。计算集群主要是负责各种复杂的计算，包括模型构建、模型更新、用户个人信息信任值计算、登录时间验证、登录设备验证等。数据库服务器则用于存储各类数据， 包括用于操作行为特征库、用户信任值、数据缓存等。

客户端则是对于整个隐私保护系统效果的呈现，客户端与服务端使用volley框架进行信息传输，功能包括用户登录注册，好友关系，发布微博，用户信息查询等。

客户端每次向服务端发送请求时都会同步自己的终端IMEI和时间，以便服务端对每次操作进行识别与更新。

# 第三章 作品测试与分析

3.1 测试方案

为了验证本文提出的信任计算模型的有效性和信任计算框架的可行性，我们以新浪微博的约150万条大数据为基础进行了一系列的实验，事实证明由该模型分类后的数据具有较高的准确率，同时信任计算框架中的各个部分都可以在实际的社交网络环境中实现。实验机器的参数如下。

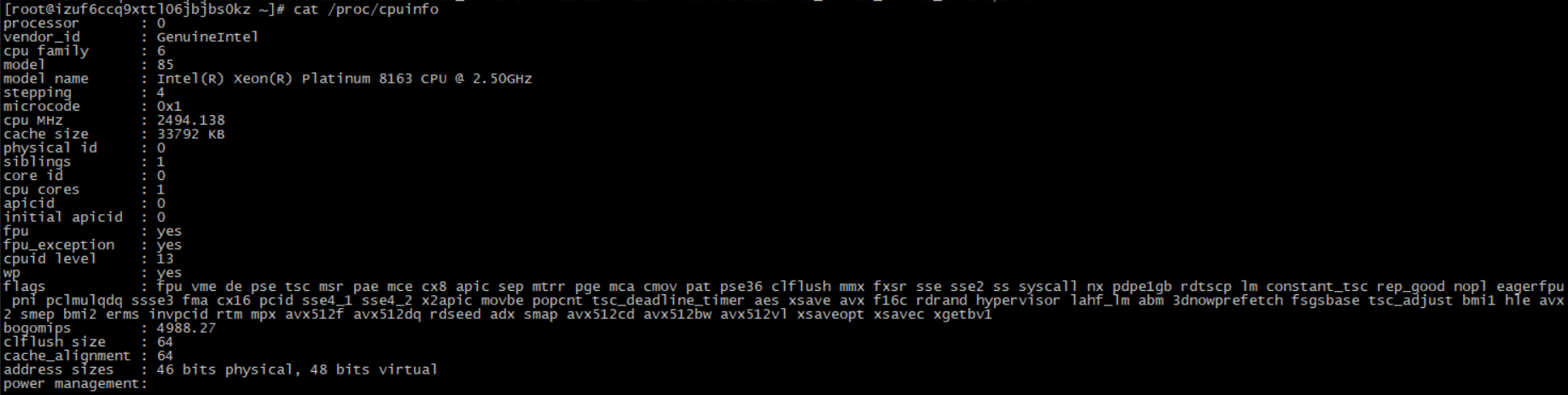


图3.1 试验机器参数

考虑到新浪微博是国内具有代表性的社交网络平台，本实验将从新浪微博中获取数据，并从中计算用户间的信任级别。根据信任计算模型的原理和信任计算框架的设计，本实验在真实的社交网络环境中实现了数据收集、数据清洗、数据分析与评价等模块，验证了信任计算框架的信任计算功能。下面就各个部分的实现细节做详细的论述。

3.2 测试数据

3.2.1 数据收集与储存

数据收集模块的目标是通过调查获取用户的信任级别，因此我们采用scrapy爬虫框架，采集新浪微博中用户信息数据存储在MongoDB中，并进行数据预处理与特征提取。数据库设置 Information、Tweets、Follows、Fans四张表，此处仅介绍前面两张表的字段。

***Information 表：***

***\_id：采用 “用户ID” 作为唯一标识***

***Birthday：出生日期***

***City：所在城市***

***Gender：性别***

***Marriage：婚姻状况***

***NickName：微博昵称***

***Num\_Fans：粉丝数量***

***Num\_Follows：关注数量***

***Num\_Tweets：已发微博数量***

***Province：所在省份***

***Signature：个性签名***

***URL：微博的个人首页***

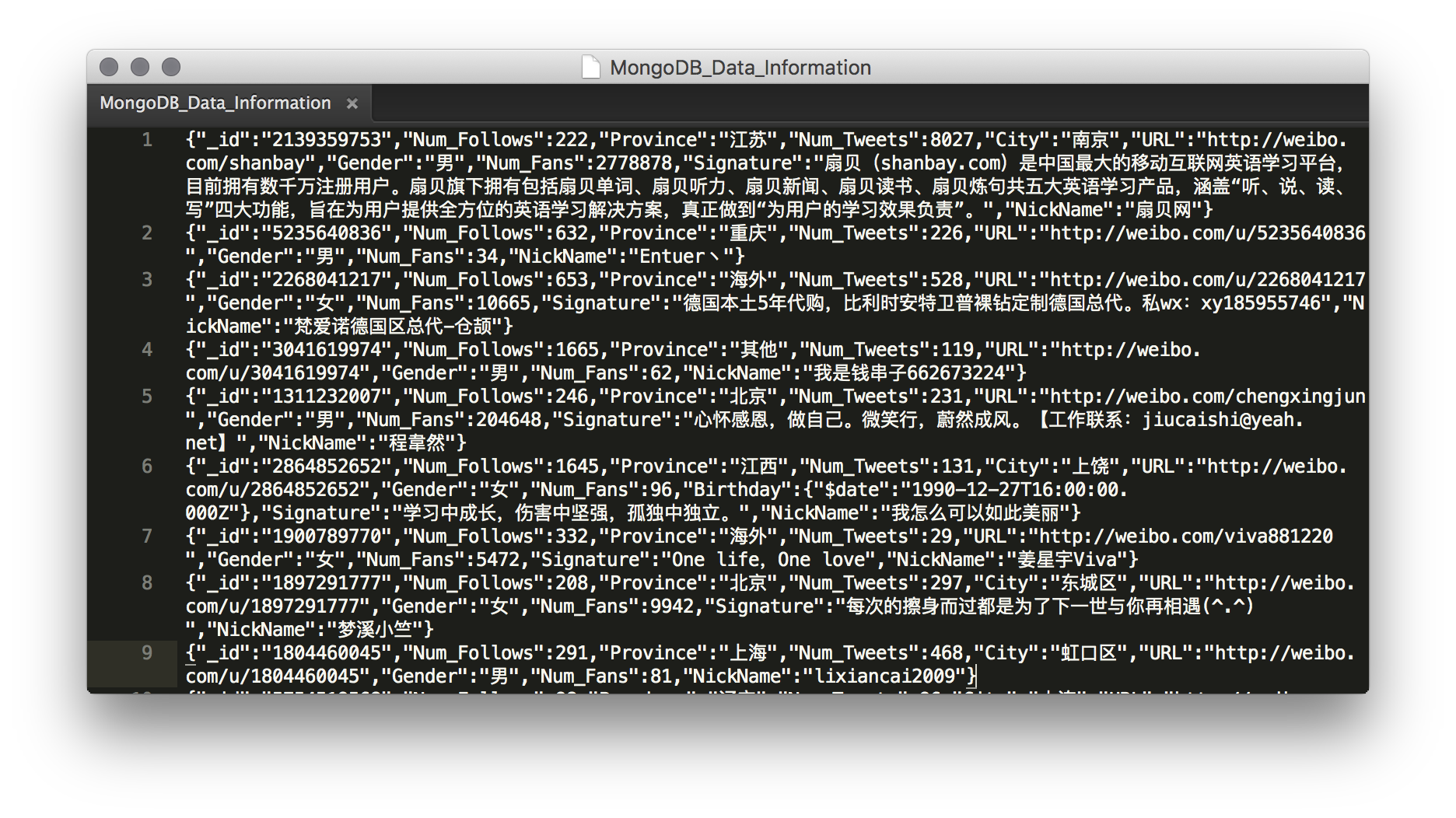


图3.2 Information表数据

***Tweets 表：***

***\_id：采用 “用户ID-微博ID” 的形式作为一条微博的唯一标识***

***Co\_oridinates：发微博时的定位坐标（经纬度），调用地图API可直接查看具体方位***

***Comment：微博被评论的数量***

***Content：微博的内容***

***ID：用户ID***

***Like：微博被点赞的数量。***

***PubTime：微博发表时间。***

***Tools：发微博的工具（手机类型或者平台）***

***Transfer：微博被转发的数量***

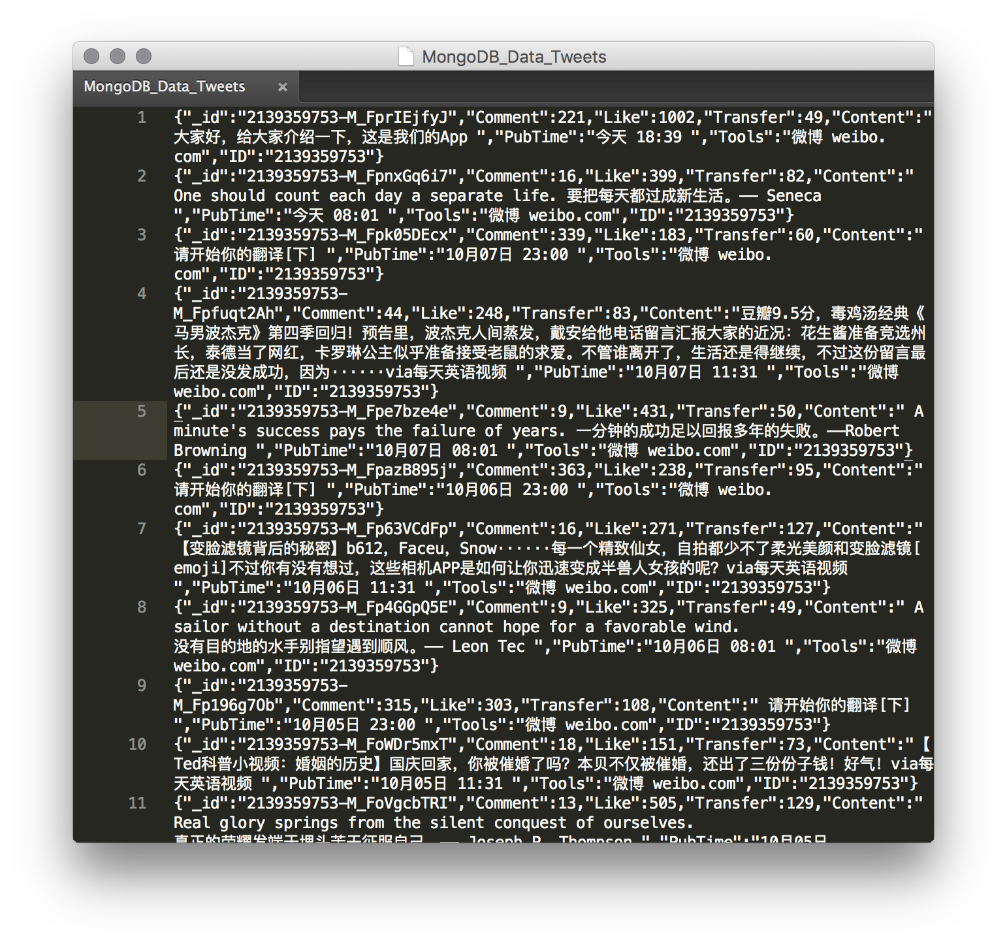


图3.3 Tweets表数据

我们使用scrapy框架，通过构建ip池与cookies池等方式对抗反爬措施，爬取新浪微博用户信息，将爬取下来的用户信息存储在MongoDB中，如图3.4所示。

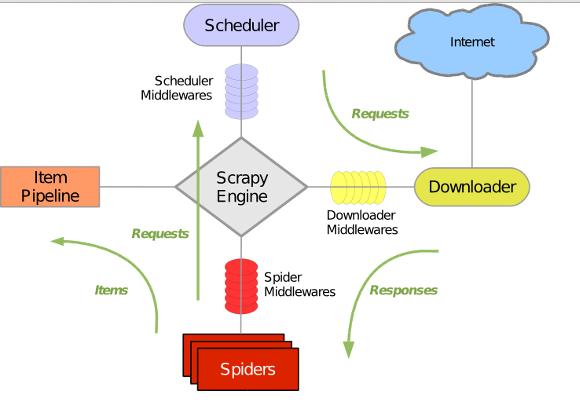


图3.4 Scrapy框架原理

3.2.2 数据清洗

紧接着对抓取到的数据进行预处理，通过数据清洗删除含有的特殊字，删除未公开个人信息的用户信息和删除关键信息不完整的用户或微博以保证获取到的用户信息具有实验价值以及保证接下来的数据分析能够顺利进行。数据清洗完毕后即可进行行为特征提取以建立特征数据库。

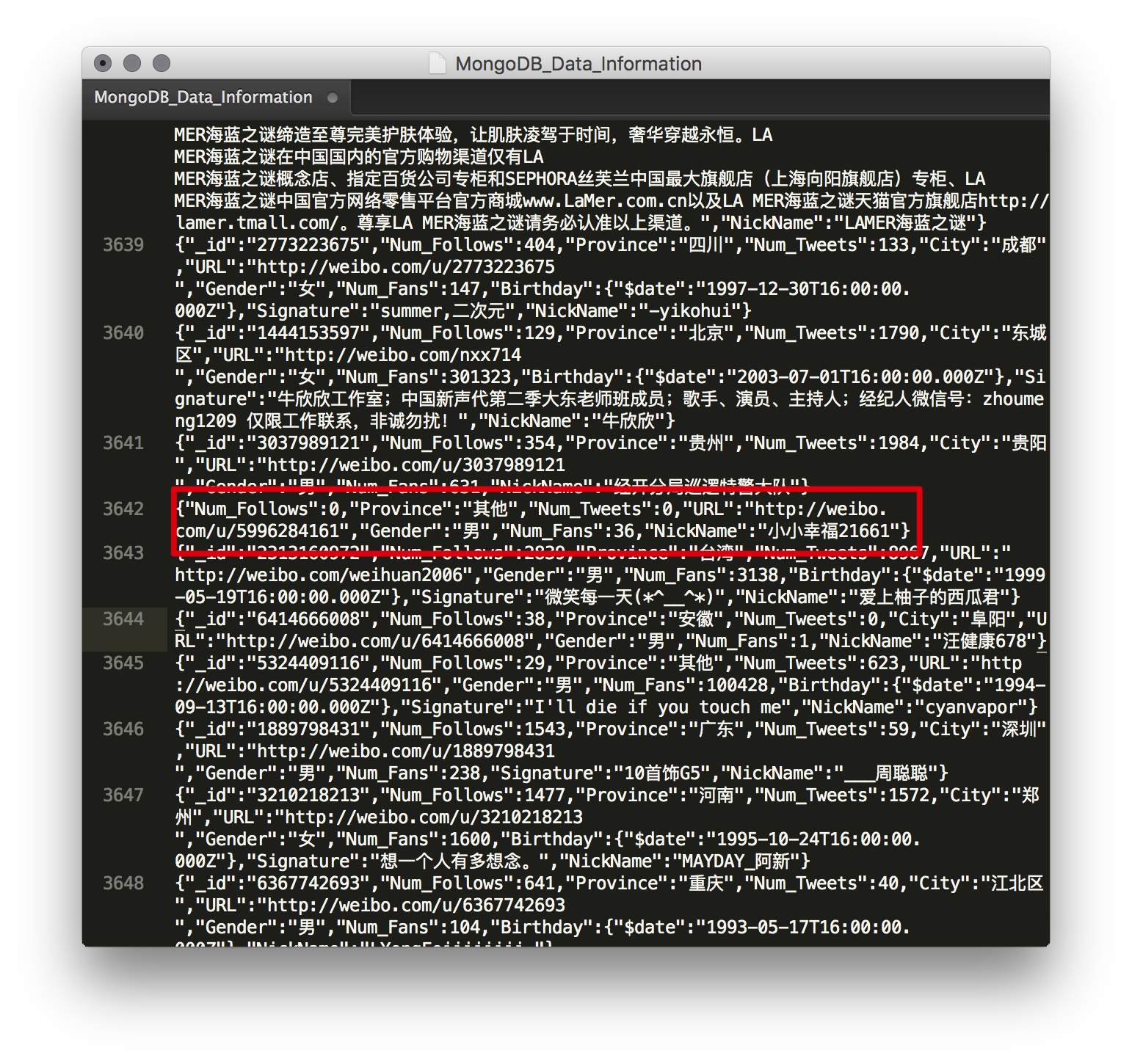


图3.5 数据样本清洗

如图3.5中框选的用户信息数据，从该数据中我们无法找到数据的索引项\_id，无法在之后的工作中进行分析，故数据清洗时将其删除以免在之后的数据分析时造成不必要的麻烦。

3.2.2 数据分析

1. 信息完整度

本次测试首先挑选了个人信息打分最高的用户，如图3.6，可以直观的看到其信息完整度非常高，所有信息都有填写。

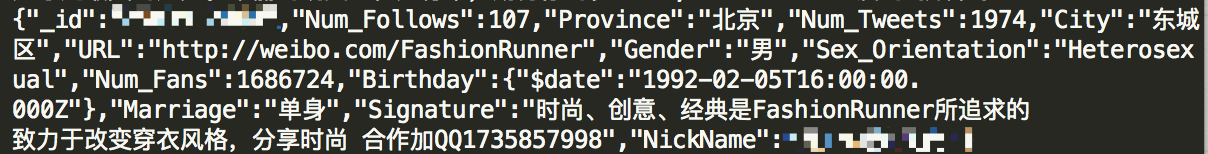


图3.6 个人信息数据样本1

第二次挑选了个人信息打分最低的用户，如图3.7，可以看出其个人信息都未填写，使用的昵称也是系统的默认昵称。



图3.7 个人信息数据样本2

1. 内容相似度

为了避免用户通过大量重复发送类似微博来提高信任值，模型引入了对微博内容相似度的检测。通过检测用户发送微博内容的相似度，对大量发送较高相似度微博的用户进行扣分处理，即用内容相似度的程度弱化微博转评赞带来的分数提高，相似度越高，弱化越强。

测试过程中，若计算用户的每一条微博与其他微博的相似度，将会产生O(n2)的时间复杂度，对于微博量很大的用户，计算时间将过长。所以模型设计为最多随机抽取该用户的20条微博进行相似度对比，求平均值后得其相似度。

在测试了随机抽样的200名用户内容相似度后，挑选了相似度较高和较低的用户微博进行查看。

如图3.8是一个微博相似度只有0.367的用户，其微博内容相似度较低，且无恶意刷微博涨信任值的迹象，信任分数提升因内容相似度带来的弱化应该非常小。为此，模型引入了相似度平方惩罚机制，使得正常发微博的低重复度弱化效果尽可能小。

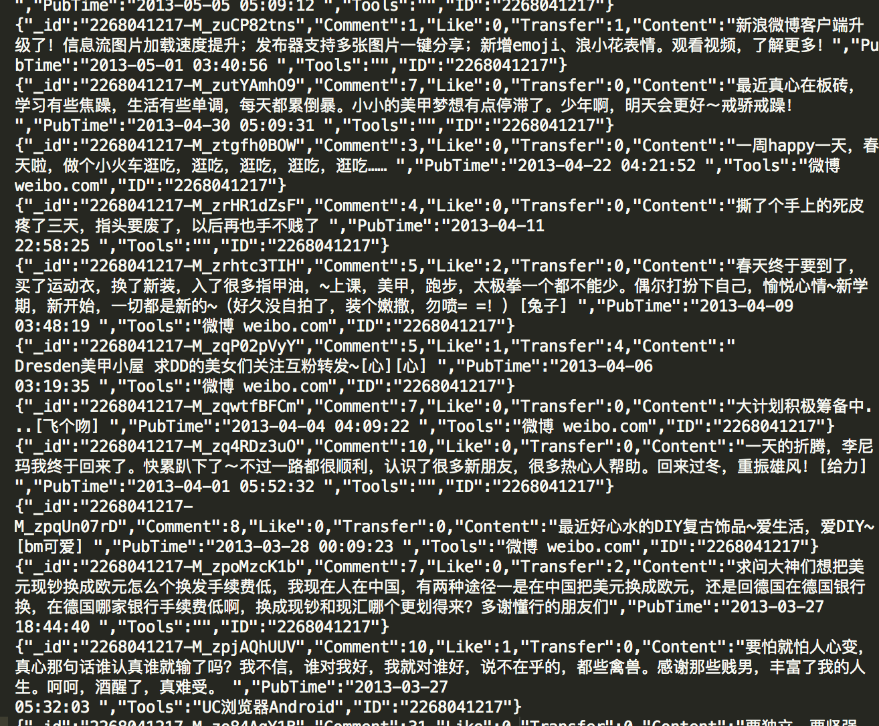


图3.8 内容相似度比较

如图3.9是一个相似度为1的用户，即抽样显示其微博内容完全一样，其类似广告的内容相似证明了模型的正确性，我们需要对其进行较强的信任分数弱化操作。

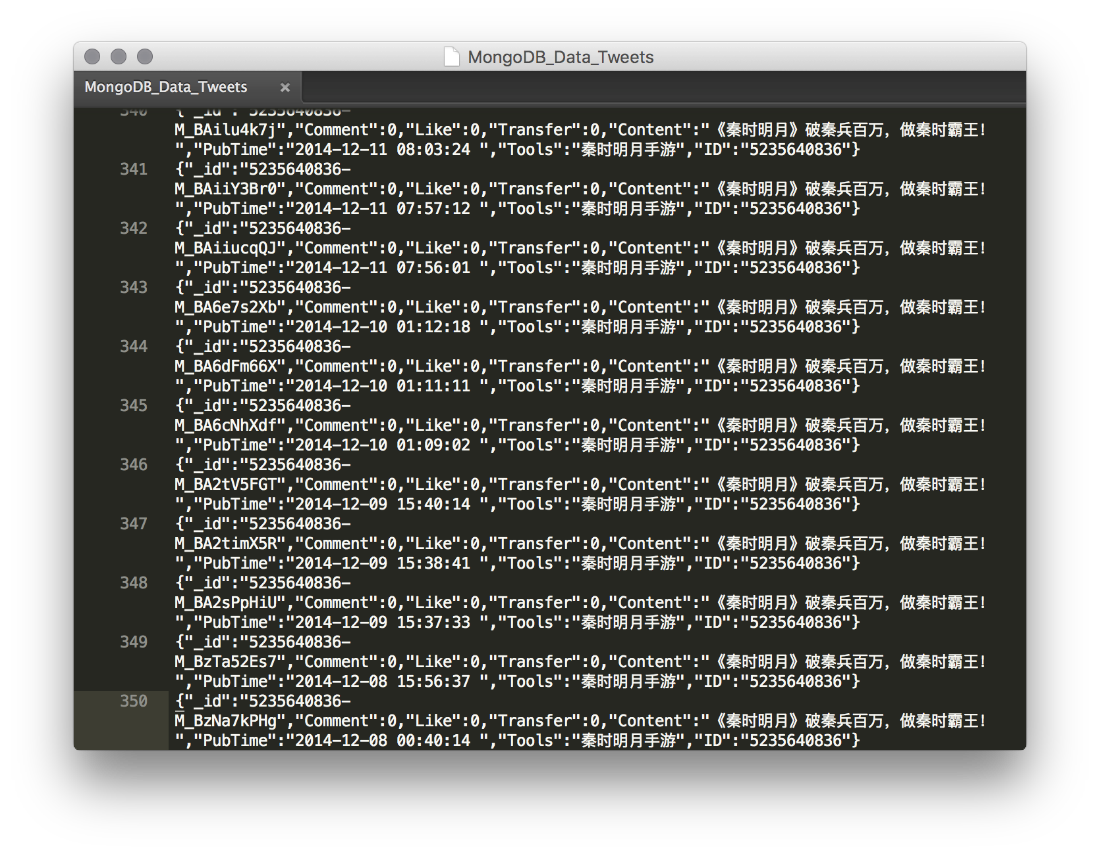


图3.9 内容相似度比较

1. 微博时间聚类

本测试最初使用45万条微博的数据集进行时间聚类，并将每个用户聚类得到的该用户的三个时间储存，在每天0点进行重新计算更新。然后计算出每条微博距离该用户的三个聚类中心的误差，并将所有误差汇总按照误差大小排序后，使用有序样本聚类将数据分为两类。当k=2时，画出的图像如图3.10所示，红色的点为超出阈值的偏差数量，蓝色的点为未超出阈值的偏差数量。即红色的点为非正常登录，其偏差较大但个数较少。超出阈值的偏差个数之和只占总数据量的约10%，是一个比较正常的数值。如果阈值过大，会导致隐私保护不够，阈值过小又会频繁提示用户验证，影响用户使用体验。

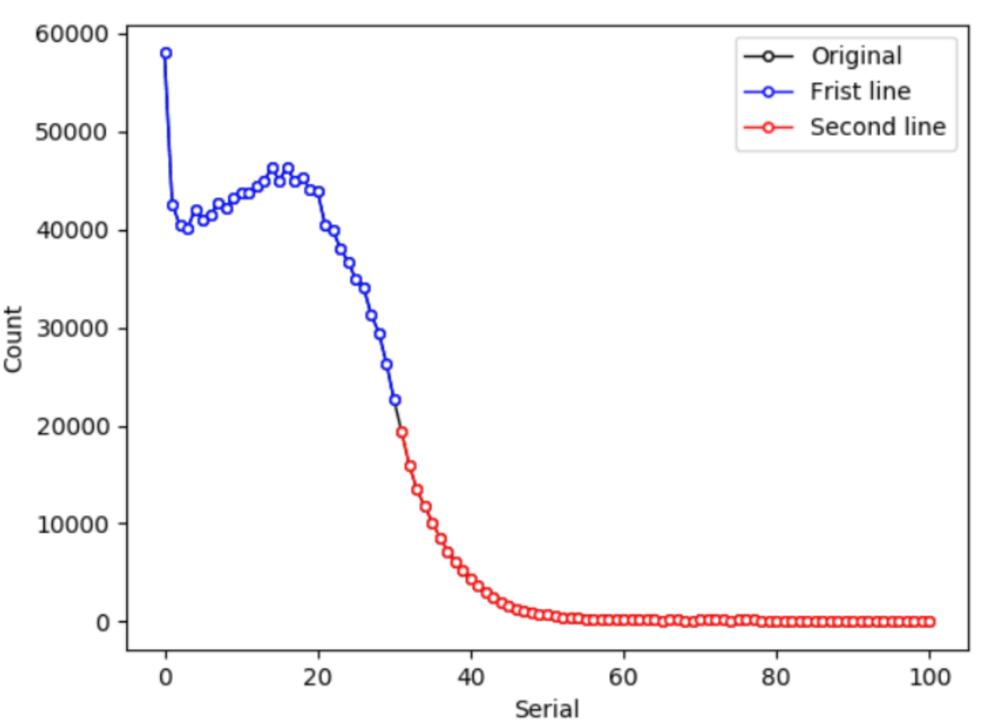


图3.10 初始时间聚类结果

如果将数据集增大到约150万条微博，做出和上述相同的操作，得到的图形(如图3.11所示)和之前几乎一样，且异常偏差数量依旧为总数据量的10%左右，证明大数据的偏差分布具有很强的规律可循。

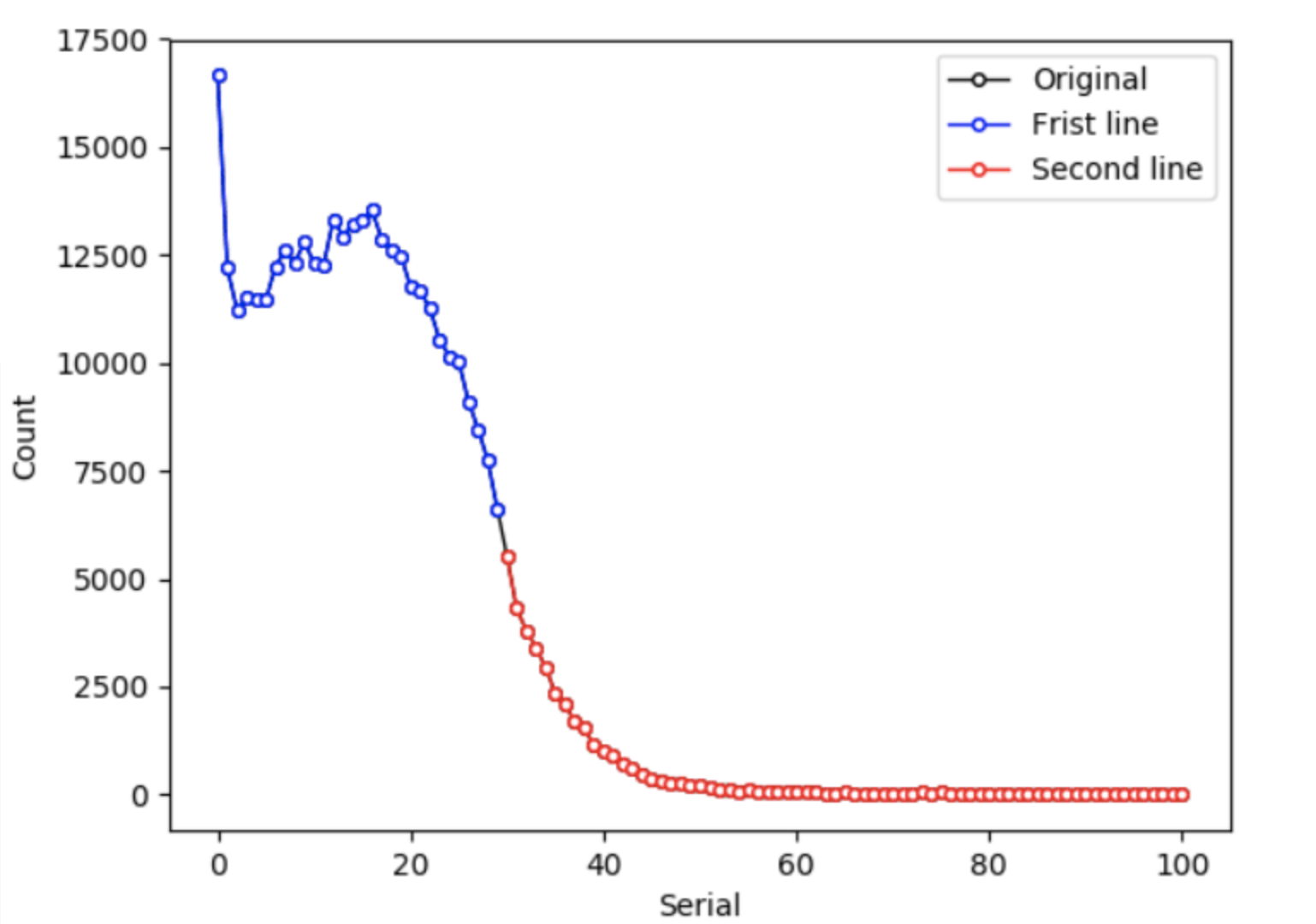


图3.11 K值对时间聚类结果的影响

若修改聚类参数k=3，异常偏差数量只占总量1%(如图3.12所示)，这将导致阈值过大，使隐私保护不够。若修改聚类参数k=1.5，异常偏差数量占总量34%，即1/3的几率会需要在用户登录时进行安全验证，所以阈值过小会影响用户使用体验。

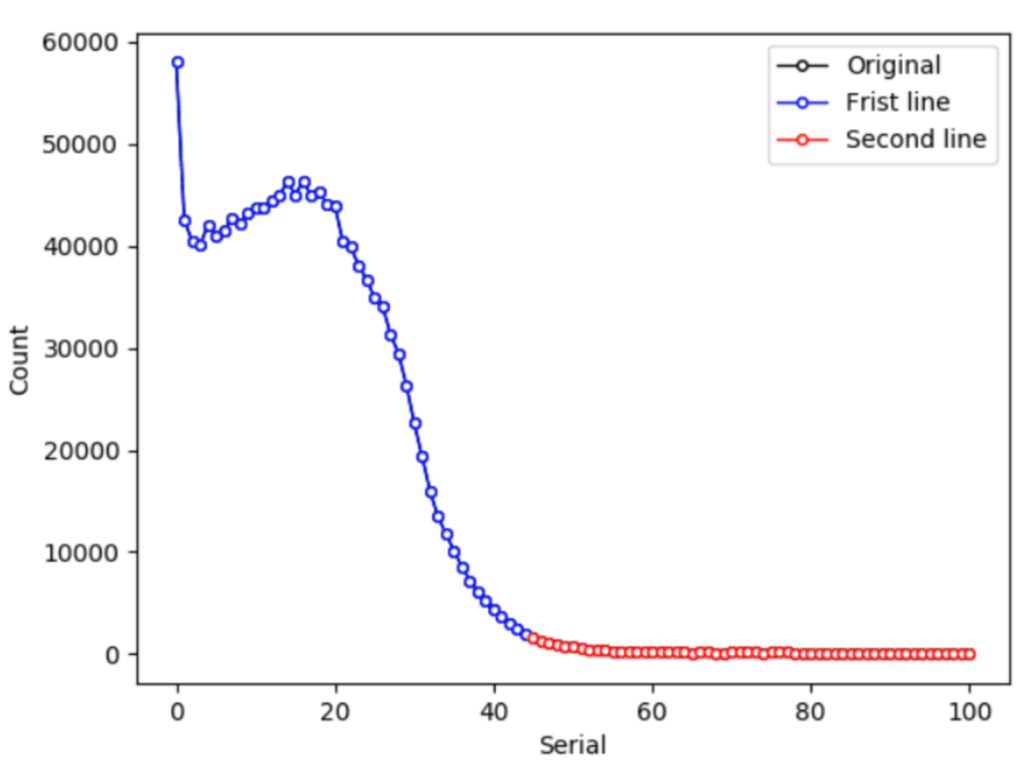


图3.12 K值对时间聚类结果的影响

任取用户进行登录测试，可得到其登录误差，在和阈值对比后可判断其是否正常登录(如图3.13所示)。若检测为异常时间登录时，将会要求其进行额外的验证(如手机验证码验证)保证用户的账号安全。

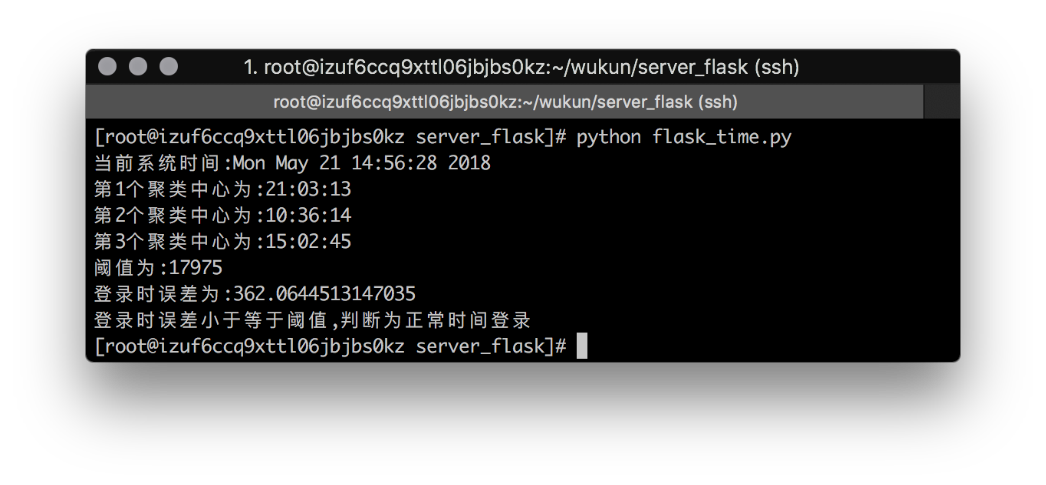


图3.13 登录测试结果

1. 遗忘曲线

由于用户最近发过的微博应对信任值产生更大的影响，需要在模型中引入了遗忘曲线。本实验测试了3种不同的参数k，当指数k取0.07时，得到的曲线符合预期要求。即开始时微博影响下降的相对较快，经过一天的时间下降到约80%，在十天后下降到一半，在一个月后下降到40%左右的水平(即图3.14中的l1曲线)。

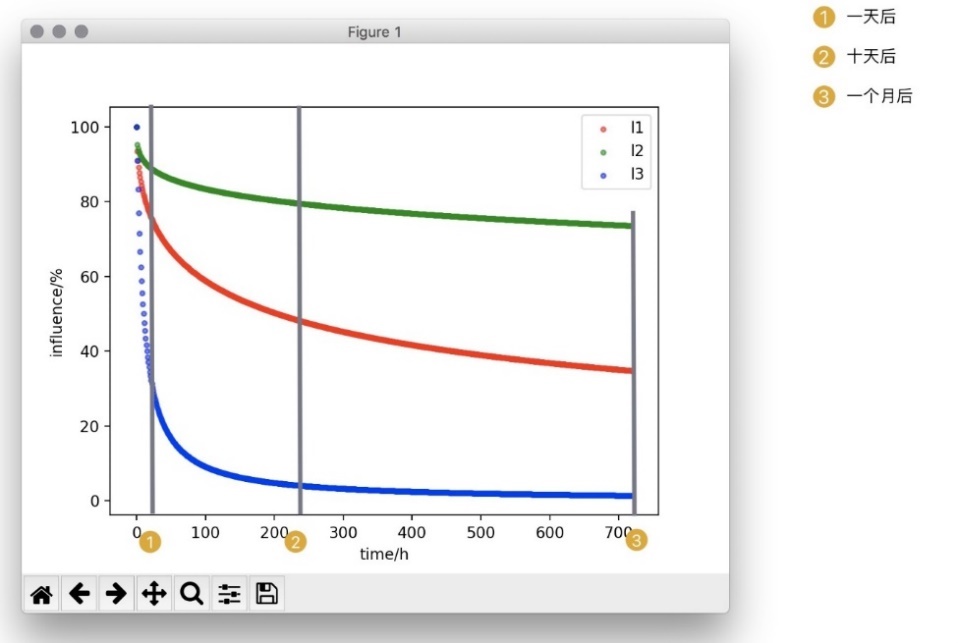


图3.14 遗忘曲线测试结果

通过这种方法得到的得分使得打分时较新的微博权重较高，较老的微博的得分也不会被完全忽略，使得活跃的”微博新人”可以很快得到较高的信任值来畅享完整信息的微博体验，一段时间不发微博的资深微博用户信任值也不会有太大下降。

1. PageRank

使用随机抽样的方法抽取数据库中200名用户样本进行PageRank测试，将其fans和follows的指向关系构成链接投票，计算出每个用户的PR值。

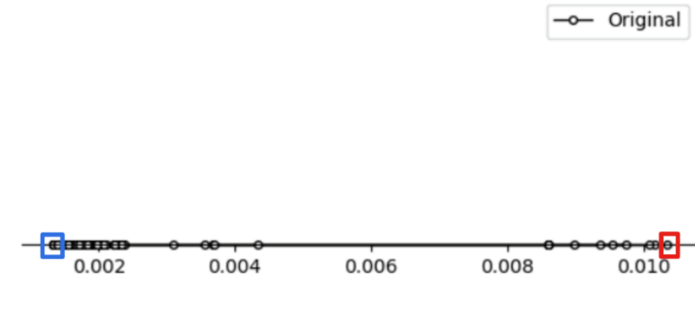


图3.15 PageRank测试结果

我们找出了图3.14样本中PR值最大的用户和PR值最小的用户，查询其id和对应的用户信息，可以直观的得到PR值大的用户被关注量非常大，而PR值小的用户被关注量确实也非常小。仔细查看PR值大的用户的粉丝也能找到不少较大PR值的粉丝，即可基本排除”刷粉”可能。我们即可用PR值作为一个依据给用户信任值打分。

图3.16为样本中PR值最大的用户，其粉丝数有118万人。

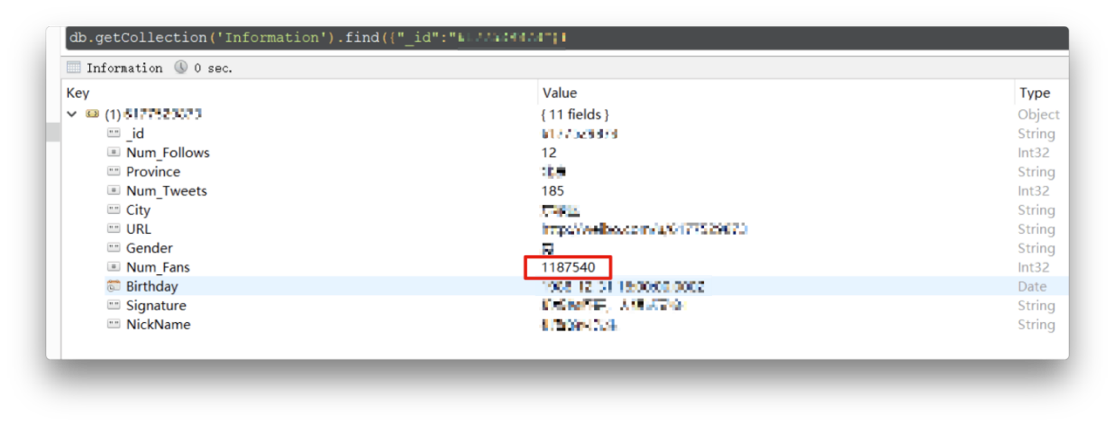


图3.16 PR值最大用户信息

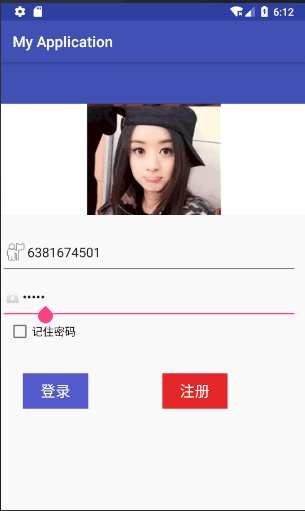
图3.17为样本中PR值最小的用户，其粉丝只有6人且这些人的PR值都较低。



图3.17 PR值最小用户信息

1. APP应用效果展示

将隐私保护系统部署在在APP服务端，客户端使用Android开发，在服务端与客户端之间使用Volley框架传输，实现了登录，注册，验证，发送微博，查看微博信息和个人信息等功能，如图3.18-3.21所示。登录阶段若用户处于危险状态（如非常用时间，非常用工具登录）则强制进行短信验证以保证用户账号安全，如图3.22所示。



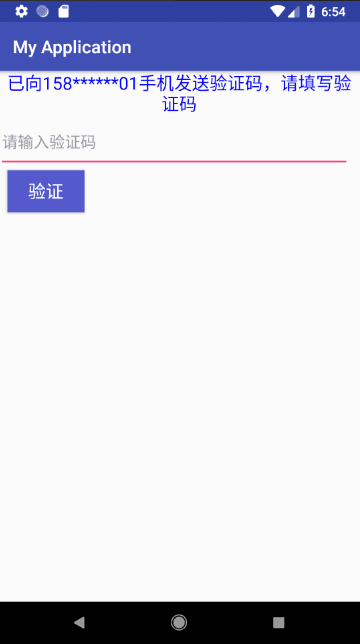


图3.18-3.22 登录、注册、发送微博、验证界面

用户在登录后服务端会根据用户信任值对用户不同请求进行不同处理：如果用户处于低信任值状态，则用户在查询信息与查询微博环节中获取到的信息将经过限制发布处理，系统将屏蔽掉信息中可能导致隐私泄露的部分，如图3.22，3.23所示，如果用户处于高信任值状态，用户的公开信息将无失真的呈现，如图3.24，3.25所示。

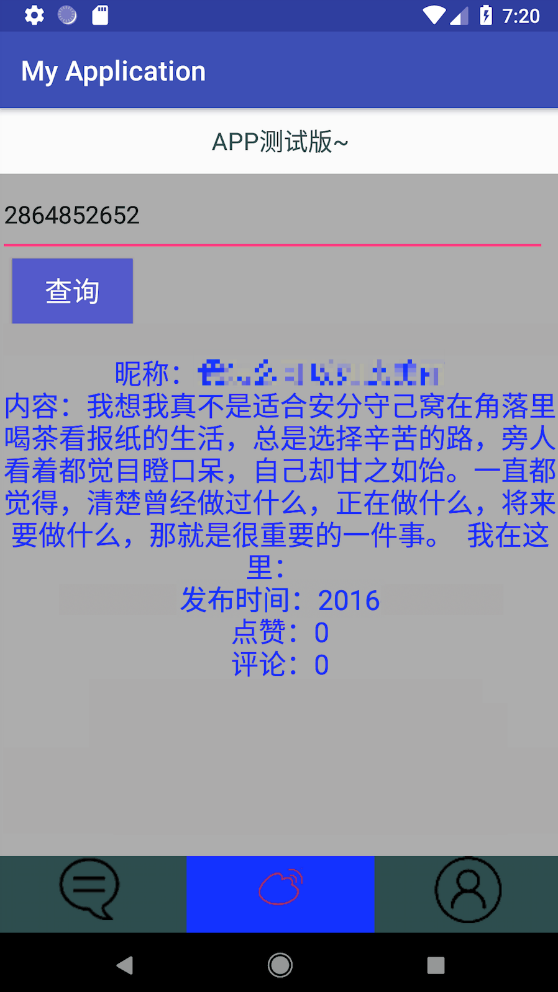
 

图3.22-3.23 低信任值用户界面

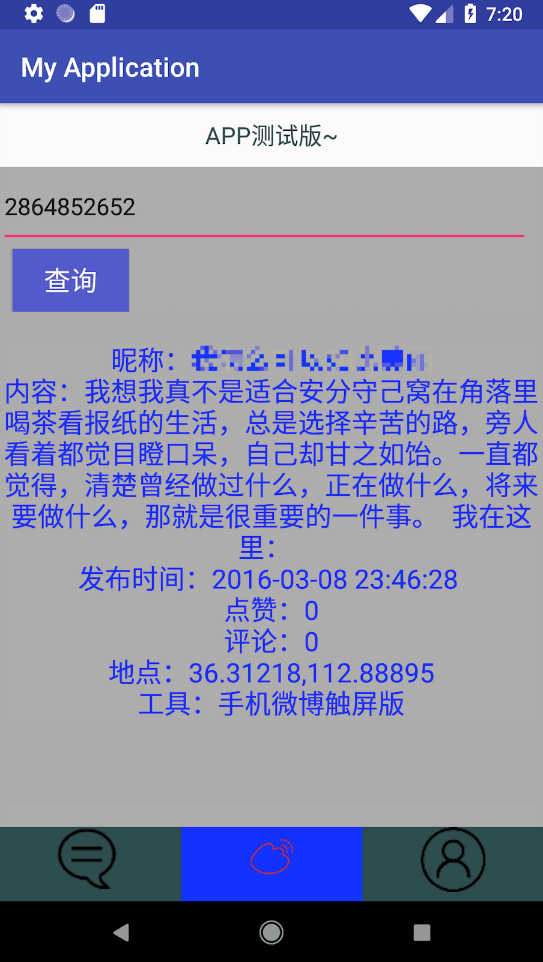
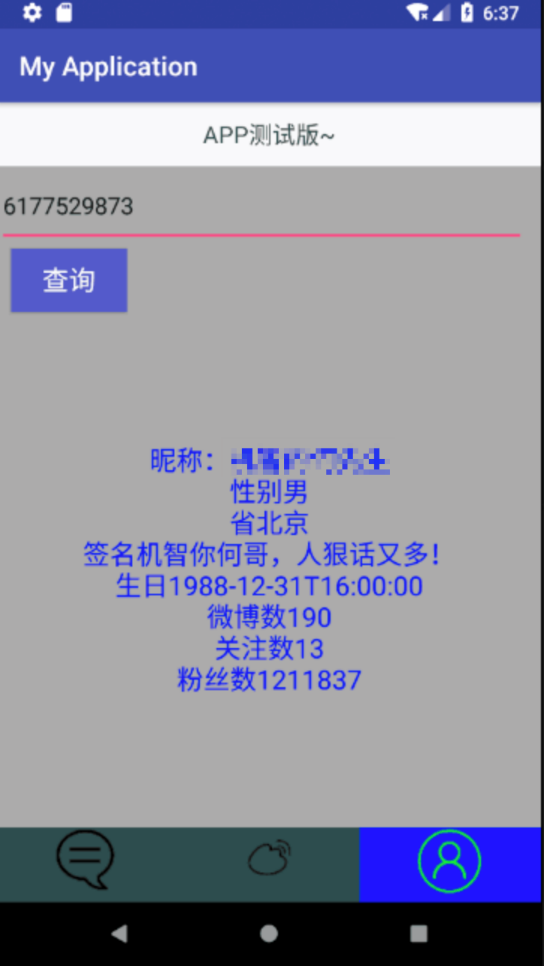
 

图3.24-3.25 高信任值用户界面

# 第四章 创新性说明

4.1 现状简述

目前对于社交网络中用户个人隐私信息的保护，主要有两种方式：一种是新浪微博及其类似应用，对于已经注册的用户，对于所有用户展示其公开的信息，一种是微信朋友圈及其类似应用，对于已经注册的用户，只对其好友展示其公开的信息。对于这两种方式而言，都存在各自的局限性。

对于第一种应用，也就是公开的信息传播于整个网络中间的应用而言，用户的个人隐私会在无意间被泄露。如下图所示，所有的用户群体都能够成功的获取到消息发布者公开到网络云上的信息，可能对于消息发布者来说，用户群体A获取到公开消息是安全的，但是用户群体B获取到公开消息对于消息发布者来说是危险的，很明显在这种模型下消息发布者处于一个危险的环境中。

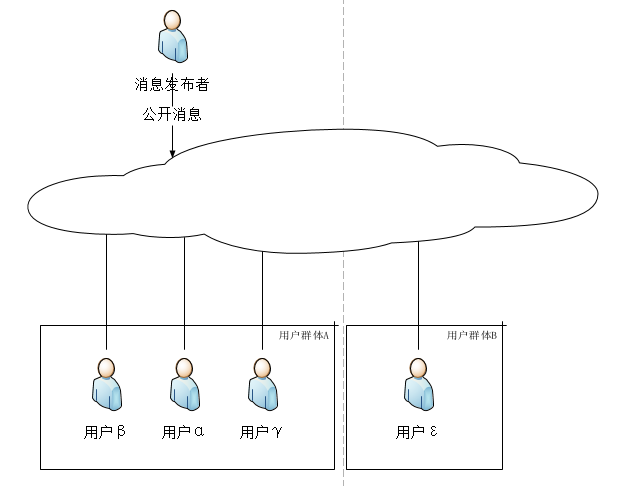


图4.1 新浪微博社交网络用户关系

对于第二种应用，也就是公开的信息之传播于某个特定群体之间的应用而言，这种模型也是现在使用比较广泛的模型。但是这种模型下，用户的个人隐私也可能在某个不确定的时间遭到窃取，同时对于用户的交流也会产生一定的阻碍。

如下图所示，对于消息发布者来说，仅仅对于用户群体A公开其信息，对其他用户群体则不公开信息，假设用户群体B对于消息发布者而言是不安全的，而群体C对于消息发布者是安全的，但是由于群体C并不处于A的群体内，所以C也不能通过合法的手段获取到消息发布者的消息，这种情况下该模型就严重影响了用户之间的正常交流过程，同时强制某用户加入群体A对于C群体的用户来说也是相当不好的使用体验。

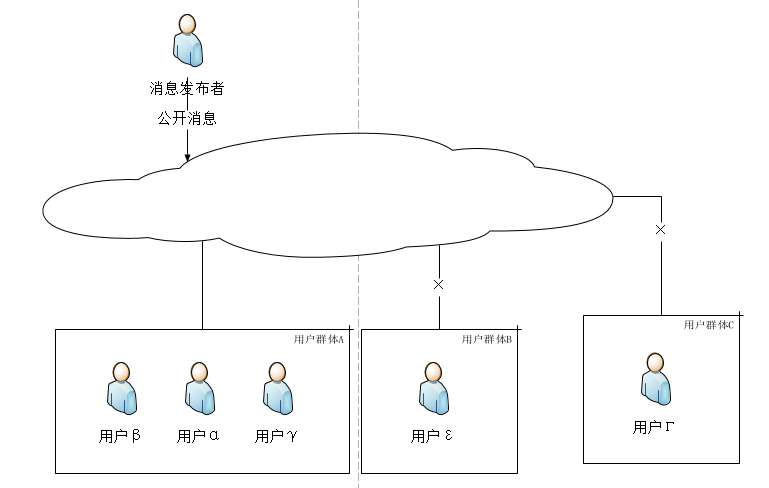


图4.2 微信朋友圈社交网络用户关系

除此之外，即使是在这样的模型当中，消息发布者也不能认为是完全安全的，如下图所示，在某个特殊的情况下，用户γ变成了用户群体B中的成员，此时用户γ对于消息发布者来说已是不安全的，但是由于消息发布者的疏忽或者是系统的不完善，不能将用户γ从群体A中删除。此时对于消息发布者而言要继续保护自身的安全就只能采用下述的两种方案之一：

1. 将所有安全用户转移到另一个用户群体中

2. 停止发布消息

第一种方案在用户群体A特别庞大时，会耗费大量的资源，而第二种方案显然也是不可以接收的。因此在这种情况下上述的根据用户群体发布消息的模型也不能很好的保障消息发布者的安全和利益。

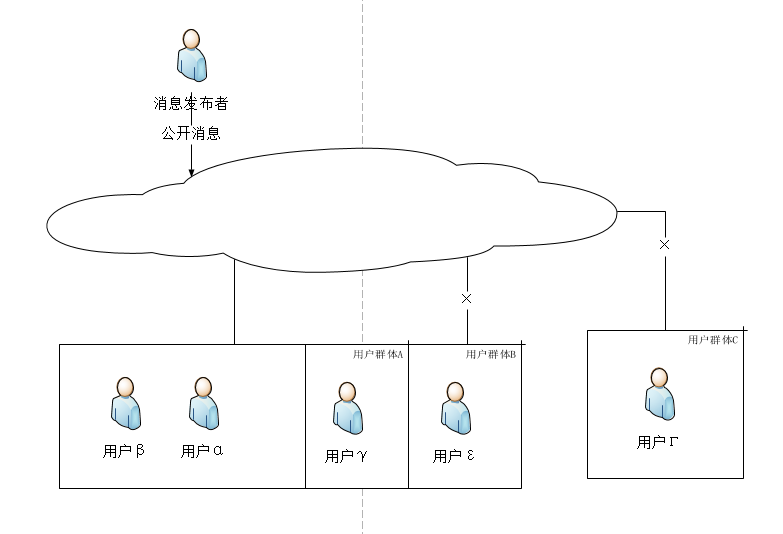


图4.3 理想状态下用户状态划分

4.2 创新性综述

本模型并未采用通过将合法用户分为不同用户群体，并根据用户群体不同给予不同权限的方式来让用户保护自己所发布的消息。而是通过系统直接识别出不安全的用户，并对于不安全用户采用限制措施的方式来保护消息发布者的安全。

如下图所示，我们将非法用户大致划分为两类，一类是用户使用他人的账号登录进行非法行为，另一类是非法用户使用自身的账号进行非法行为。

对于第一类用户来说，前一节叙述的两种访问限制模型都不能很好的保护消息发布者的信息。对于第二类用户来说，前一节叙述的第一种访问限制模型不能很好的保护发布者，第二种访问限制模型存在被破解的危险。而对于本文提出的模型来说，我们可以通过对于该账号的一些以往登录的时间、地点和设备，分析出本次登陆的安全系数，对于一次不安全的登录请求，通过采用账号验证的方式对于其账号登录操作进行限制。

对于第二类用户来说，前一节叙述的两种访问限制模型依然存在着被破解的危险。对于本文提出的模型来说，我们对于该账号的信任程度是较低的，对于信任程度较低的账号，我们对于服务器返回的数据进行一定程度的模糊化处理，这样对于消息发布者来说，也能切实保护消息发布者的合法利益。



图4.4 基于用户行为的隐私保护机制

# 第五章 总结

本作品针对当前隐私保护方法不能很好的保护移动互联网中的用户隐私数据的问题，结合移动互联网环境下用户行为的特点，提出了移动互联网中基于用户行为的隐私保护机制及其应用：首先，对移动互联网环境下用户行为进行分析与特征提取，构建访问控制模型；随后，通过网络爬虫技术获取构建访问控制模型所需要的数据，并进行预处理；接着，使用处理后的数据进行模型训练，通过对用户个人信息与行为信息进行分析计算用户信任值，实现由信任值到访问权限的映射以及访问控制模型系统；最终，将该隐私保护系统部署于仿社交平台服务端，并在客户端进行测试。

本作品主要工作包括：

1．对当前社交网络中隐私保护机制的基本概念、研究思路、研究现状与关键技术进行研究，阐述当前移动互联网环境下用户信息的结构，并对用户基本信息、用户行为信息和用户关系信息进行剖析，提出移动互联网用户信任值的计算模型。

2.选择使用人数众多、具有巨大用户关系网的新浪微博数据集作为训练样本。使用scrapy框架，通过构建ip池与cookies池等方式对抗反爬措施，爬取新浪微博用户信息，对采集到的数据进行预处理，通过测试与仿真实验验证数据集的有效性。

3.通过已有的数据搭建用户信任值计算模型，包括基于用户基本信息的信任值初始化、基于K-means聚类的异常时间检测、基于PageRank的用户关系分析、内容相似度分析和遗忘曲线信任值更新。在此基础上，引入时间与事件更新驱动机制，对用户信任值进行维护，实现了完整的从用户信息到访问安全等级的映射。

4.设计并实现了一套基于安卓5.0的安卓仿社交APP，将隐私保护系统部署于服务端，验证了基于用户行为的隐私保护机制的正确性和合理性。

本作品还可以从以下方面作进一步完善：

1.针对社交网络中用户间信任的动态变化的特点，考察与用户之间的信任变化有关的因素，建立数学模型进行描述，使得信任计算模型具备实时描述信任的能力。

2.优化隐私信息和隐私策略的描述，或在当前模型的基础上设计一些工具来简化用户进行设置的过程。

3.随着分布式计算、大数据的到来，需要利用分布式计算快速的进行模型的训练与更新、利用更高效的数据挖掘方法进行数据的处理、并发进行的K-means的计算。

4.当前的访问控制模型仍然需要一定的人工干预，未来可利用更好的机器学习算法来实现全封闭的模型更新，使得模型可以在不需要任何人工干预的情况下不断适应外界环境的变化。

# 参考文献

1. 赵康. 基于信任的社交网络隐私保护机制研究[D].上海交通大学，2015.

[2] Mirkes， E.M. ["K-means and K-medoids applet"](http://www.math.le.ac.uk/people/ag153/homepage/KmeansKmedoids/Kmeans_Kmedoids.html). Retrieved 2 January 2016.

[3] Phillips， Steven J. (2002-01-04). Mount， David M.; Stein， Clifford， eds. Acceleration of K-Means and Related Clustering Algorithms. Lecture Notes in Computer Science. Springer Berlin Heidelberg. pp. 166–177. doi:10.1007/3-540-45643-0\_13. ISBN 978-3-540-43977-6.

[4] Page， Lawrence; Brin， Sergey; Motwani， Rajeev; Winograd， Terry (1999). "The PageRank citation ranking: Bringing order to the Web". Archived from the original on 2006-04-27.， published as a technical report on January 29， 1998.

[5] 李凤华，苏铓，史国振，马建峰.访问控制模型研究进展及发展趋势[J].电子学报，2012，40(04):805-813.

[6] 孙立伟，何国辉，吴礼发.网络爬虫技术的研究[J].电脑知识与技术，2010，6(15):4112-4115.

[7] 胡启平，陈震.试析社交网络环境中的个人隐私保护[J].信息网络安全，8:43-44， 2010.

[8] J．Golbeck．Tutorial on using social trust for recommender systems．In Rec Sys 09: Proceedings of the third ACM conference on Recommender Systems，pages 425-426，New York，USA，2009．

[9] 尹光宇.社交网络中用户间信任度量模型研究[D].中国科学技术大学，2013.

[10] 乔秀全，杨春，李晓峰等．社交网络服务中一种基于用户上下文的信任度计算方法[J]．计算机学报，2011，34(12)：2403—2415．