

威海市公安局环翠分局

大数据辅助分析查询系统服务和
涉网新型行为分析系统服务

项目建设方案

申报单位：威海市公安局环翠分局

申报时间：2024 年 7 月

目录

第一章 项目背景及必要性	4
第二章 现状和需求分析	4
第三章 项目建设内容	4
3.1.大数据辅助分析系统	4
3.1.1.全息画像	4
3.1.2.WiFi 画像	7
3.1.3.基站画像	8
3.1.4.网关画像	8
3.1.5.空间提数	9
3.1.6.智能研判	9
3.2.涉网新型行为分析系统	10
3.2.1 打击反制	10
3.2.2.预警阻断	22
第四章 项目设计方案	25
4.1.总体架构及技术路线	25
4.1.1.总体架构	25
4.1.2.技术路线	26
4.2.系统拓扑图	27
4.3.网络系统设计	28
4.4.安全系统设计	28
4.4.1.网络层安全	29
4.4.2.系统层安全	29
4.4.3.应用层安全	30
4.4.4.数据层安全	31
4.5.终端系统及接口设计	31
4.6.其它系统设计	31
4.7.信息资源规划及项目形成的信息资源目录	32
4.8.云服务需求或系统软硬件配置及部署方案	32
第五章 项目组织管理	32
5.1.项目组织机构	32
1、项目领导小组:	32
2、 项目负责人	32
3、技术支持组	32
5.2.项目进度安排	33
5.3.安全管理制度	33
5.4.人员培训	33
1、培训对象	33
2、培训方式	33
3、培训内容	34
5.5.保障措施	34
(1) 不限定时间电话技术服务	34
(2) 现场开发技术服务	34
(3) 远程故障排除	35

(4) 定期巡查服务	35
(5) 技术升级服务	35
(6) 相关规范或标准变更的修改服务	35
第六章 项目投资	35
6.1.项目资金预算	35
6.2.项目资金来源和资金安排计划	38

第一章 项目背景及必要性

略。

第二章 现状和需求分析

略。

第三章 项目建设内容

3.1.大数据辅助分析系统

3.1.1.全息画像

全息画像要具有通过对目标设备的线上数据进行分析，掌握目标的行为点位，建立画像。

1、特征码信息

我局使用者可通过特定目标的设备的任何一个特征码，获得其它特征码的信息，从而为分析特定目标提供信息支撑。通过输入手机号码、设备 MAC 码、IMSI 国际移动用户识别码、IMEI 移动设备国际身份码、IDFA 苹果广告识别码、OAID 安卓广告识别码、ICCID 设备 SIM 卡号码、安卓 ID 码任意一个特征码获取其他码信息，实现特征码互译。

查询关联设备，获取目标设备可能的设备和换机换卡情况。

查询设备信息，获取目标设备的基础信息如设备机型、设备语言，其他特征码信息。

查询卡码关联情况，根据数据汇报进行逻辑计算推测手机号

码和 IMSI 卡关联强弱关系。

查询设备历史汇报情况，通过时间轴方式直观展示设备关联手机号码、IMSI 卡码的历史使用情况。

2、画像推测

要求系统对特定目标的画像进行推测，按照基础信息、地区信息、出现点位、特征标签、备注信息五个维度进行展示，包括性别、年龄、原户籍地、居住地、工作地、最新点位以及特征标签等画像信息。

3、线上行为

要求通过对指定设备的 APP 应用情况进行查询，系统将自动对 APP 进行敏感程度的分类，公安机关可根据设备中各类应用分级分类情况、应用安装卸载情况、应用活跃情况、开发者情况等信息，进一步分析该设备使用人的上网习惯。

APP 分类：敏感 APP 应用、小众 APP 应用、其他 APP 应用。

APP 应用使用情况：历史安装应用、目前安装应用。

APP 应用详情：应用名称、图标、包名、应用分类、安装时间、卸载时间、卸载次数、活跃时间等。

根据线上行为查询结果，我们可进一步判断目标设备使用人的兴趣爱好、违法违规可疑行为，并进一步分析其违法上网工具。

4、常连 WiFi

要求系统自动获取并分析指定设备近 30 天经常连接的 WiFi 热点信息，并将白天和晚上常连的 WiFi 点位进行展示，并具有查询在 WiFi 热点下的同网设备情况。

WiFi 热点查询：显示常连 WiFi 类型、WiFi 名称、WiFi 设备 MAC 码、WiFi 分类、WiFi 所在位置、经纬度、连接天数。

同网设备情况：设备 ID、设备机型、目标画像、连接 WiFi 及天数、特征标签等。

要求通过对目标人常用设备的常连 WiFi 查询，可快速锁定嫌疑人员白天或夜晚常出没的地点，对于我局的落地抓捕工作将起到巨大的辅助作用。

5、关系图谱

根据查询某段时间内目标设备连接 WiFi 的情况，要求可以查看与设备同网络的其他设备（含移动设备和非移动设备），并可灵活设置同网时间条件，分析各设备间的同网关系，快速判断出与特定查询对象关系密切的设备，实现对特定目标关系的挖掘。

目标设备常连 WiFi 信息: WiFi 名称、WiFi 设备 MAC 码、WiFi 类别、风险标签、WiFi 位置、连接次数、同网时间等。

同网设备详情: 目标 WiFi 同网设备关系图谱、设备信息、设备连接详情。

6、历史 IP

要求能够展示设备关联的历史 IP 信息，涵盖基站 IP、宽带 IP、运营商节点等。关联的 IP 信息包含首次关联时间、末次关联时间、IP 地址、IP 类型、运营商等，并可以将关联的信息导出。

7、点位管理

要求系统通过一张图的方式，展示地图上描绘指定的目标设备在一定时间范围内的点位信息，实现点位分析和历史点位回溯功能。提供时间、点位描述以及地图描点等方式显示目标的出现点位，便于快速锁定设备的点位。

可自动分析判断目标设备出现的点位、近期的落脚点、工作地和居住地信息。

地图类型具有百度离线地图、卫星离线地图，具有对地图的测距、标记、圈选、地址查询等功能。

具有点位聚合，点位信息的查询。

具有 GPS、WiFi、基站等多维度点位信息。

8、点位分析

根据目标设备的历史点位，要求自动分析判断目标设备最近出现的点位、近期的落脚点、工作地和居住地信息。

最新点位：最近一次出现的时间和点位。

地区：原籍地、居住地、工作地。

停驻地：停留一段时间范围下的点位，包括出现频率，停留时间，出现时间。

城市：按出现时间排序停留的城市和停留的时间。

9、关联基站

通过对目标设备的关联基站进行查询，要求可查看设备连接的基站和连接时间。批量选中基站信息后，可查看基站画像热力情况。在实际应用中当设备机主篡改设备点位错误显示设备点位信息时，可通过关联基站功能进行真实点位校准。

具有基站筛选：运营商、基站号、关联时间、城市。

展示关联基站信息：关联时间、基站号、运营商、最新点位，查看基站画像。

3.1.2.WiFi 画像

要求通过搜索 WiFi 设备的名称或设备 MAC 码，对指定时间内连接指定 WiFi 的设备进行查询筛选，查看该 WiFi 的画像信息。同时可查看该 WiFi 设备下关联的设备信息、附近 WiFi 信息、历史关联 IP、历史点位等信息。

通过对 WiFi 设备的画像查询，可有效针对可疑窝点情况进行探测，了解该点位下常联设备、窝点迁移情况、周边其他可疑窝点情况扩线，为案件侦破落地提供信息拓展和研判手段。

WiFi 画像信息包括：WiFi 名称、WiFi 设备 MAC 码、最新点

位、风险属性等。

关联设备信息：设备图谱关系、设备基本信息，具有选择对连接或扫描的设备进行关联。

历史关联 IP 可查询到一段时间内该 WiFi 连接过的 IP 地址、IP 类型、运营商等信息。

历史点位可查询到 WiFi 点位的变更情况，便于有效发现窝点迁移行为。

3.1.3.基站画像

在我们侦查办案过程中，往往能够获得可疑目标设备连接过的基站信息，但传统的基站定位，只会给出基站的位置区码，没有办法通过可视化的方式看到可疑目标所处的区域，基站画像功能可通过输入基站号在地图上可视化的展示基站信息，帮助我们快速确定基站覆盖区域、辅助研判可疑目标的具体所处区域。

要求具有单独查询或批量查询基站信息。

要求具有查询移动、联通、电信等运营商基站信息。

查看基站基础属性、基站覆盖热力图。

3.1.4.网关画像

要求系统具有通过网关 MAC 快速查询网关的关联设备、关联 WiFi、网关最新位置、网关历史位置、网关风险属性等信息，能极大提高设备的同网扩线能力。针对关联出的设备可在图上进行手动聚合、删除 WiFi、删选设备等操作；针对关联 WiFi 可展示目标网关所关联过的所有 WiFi 信息，包含 WiFi 名称、WiFi MAC、风险标签、WiFi 分类、WiFi 位置等信息；网关的历史位置可查询网关在指定时间范围内，连接该网关的设备上报的位置。通过聚合判断可以判断出窝点有无搬迁行为。如当研判人员需要扩线

同网设备时，可以利用网关画像进行分析。如一个电诈团伙有多个办公室，且路由器都是桥接的情况，研判人员可以结合已掌握的一个 WiFi 找到对应网关，通过网关画像把多个办公室其他的设备拓展出来。

3.1.5.空间提数

1、围栏提数

我局可新建围栏提数任务，在指定的区域和时间段范围内，通过各种筛选条件进行快速提数，从而达到快速缩小排查范围，辅助我们能快速定位到可疑设备，节约宝贵的警力和办案时间的目的。

提数筛选条件：性别、年龄、消费水平、设备品牌、设备语言、安装特定 APP、经纬度等。

2、基站提数

通过输入基站号，可对指定时间内连接指定基站的设备进行查询筛选，查询连接设备信息。系统具有秒级查询并展示设备信息，展示筛选条件、基站信息、查询结果信息。

筛选条件：具有对有无 sim 卡、时间段、性别、年龄范围进行筛选提数。

基站信息：所在点位、经纬度。

查询结果：设备特征码、机型、基本信息、连接时间、特征标签、原籍地、常驻地等。

3.1.6.智能研判

1、WiFi 碰撞

根据实战，提取多个 WiFi 不同时间段下的连接、扫描的设备，可针对发现嫌疑人具有多时、多地活动的情况时，提取多个

WiFi 进行碰撞产生数据交集，具备分析出与多个目标 WiFi 关联的设备的功能，缩小侦查范围，发现嫌疑目标。

在系统中可以对多个不同时间段下的不同 WiFi，对连接、扫描该 WiFi 的设备采用取交集或者并集的方式计算出符合条件的关联设备，包含设备 ID、设备扫描、连接的 WiFi、连接次数、扫描次数及原籍地、常驻地等信息；同时具有碰撞结果的导出。

2、全息批查

当案件侦破中，需要在案件中查询多个设备的全息画像时，如果采用逐个查询设备信息时，会导致工作量大影响工作效率。所以开发全息批查功能，可以一次性查询最多 50 个设备的全息画像，查询结果包含 APP 列表、位置轨迹、常连 WiFi、关系图谱等内容，并可导出查询结果。

3.2.涉网新型行为分析系统

3.2.1 打击反制

通过移动互联网大数据资源与全域定位能力，综合研判可疑应用信息和涉网新型犯罪团伙，并辅助我们溯源、打击和反制。

3.2.1.1.应用管理

对通过报案信息、用户上传等途径上传到平台的所有可疑应用进行管理。具有通过应用中文名、包名、涉案类型、应用来源等筛选可疑应用，并可直接对选中的可疑应用进行 APP 分析，同时具有 APK 批量导出，帮助进一步辅助研判。

针对每一款应用建立了 APP 画像，通过证书信息、域名信息等应用特征，计算同源 APP 情况，展示同源 APP 列表以及每款 APP 应用报告。

3.2.1.2.模型智库

根据大量实战经验，不同类型的电诈案件中，作案人员使用的工作机在 APP 安装、活动轨迹等方面均存在特征，例如“杀猪盘”类案件的作案人员，通常会安装大量婚恋交友、位置伪装、恋爱话术、手机银行类 APP，在活动规律及画像上存高危原籍地、往返境内外、到访高危地区、频繁更换手机卡等特征；同时，作案窝点及窝点内的 WiFi 也会存在明显特征，例如大量中低端品牌手机长期同连一个 WiFi 热点且长期保持充电状态、同一 WiFi 下连接的手机设备均大量安装上述几类 APP 等。

系统具有根据上述特征，利用特征建模技术，建立 GOIP 设备发现、WiFi 聚集模型、杀猪盘窝点模型、APP 运营开发者窝点模型、境外九国跨境模型等实战模型，实时扫描辖区内活动的移动终端设备，及时发现符合模型特征的设备、WiFi 和窝点，主动进行线索推送，具有以地图的形式展示推送人员的最新位置、家庭地、工作地等信息，模型算法逻辑根据实际电诈态势长期优化，数据定期更新。

3.2.1.3.智能应用

系统具有提供多种智能应用方向功能，是对反诈工作中技战法的一种应用，包括资金链预警分类、境外围栏提数、设备同网扩线、WIFI 同网扩线等。

1、资金流预警分类

资金流预警是目前反诈工作中很重要的一环，预警线索来源较多，线索中含有受害人数据以及嫌疑人数据，实际工作中要快速识别受害人群体然后进行精准劝阻。基于资金流预警数据，将数据中的 PN 以及其他设备 ID 导入到本系统中，可以快速的识别

出预警对象是潜在受害人、涉引流人员或涉网赌人员等，通过区分可以减少反诈民警的工作量以及增加劝阻对象的精准度，减少警力投入。

2、境外围栏提数

系统具有境外国家的围栏提数功能，用户可通过新建境外围栏提数任务，在用户指定的境外区域和时间段范围内，进行设备与 WIFI 信息的提数，从而达到快速缩小排查范围，辅助各级公安机关能快速定位到可疑设备，特别是诈骗分子的生活机设备，输出设备特征码、机型、特征标签、常驻地、围栏内最后出现时间等信息，从而达到节约宝贵的警力和办案时间的目的。提数结果可进行一键导出。针对围栏提数的设备信息可进行群体分析。

设备提数信息包括设备 ID、机型、特征标签、常住地、手机号归属地、围栏内最后出现时间、最新位置与时间。

WIFI 提数信息包括 WIFI 名称、WIFI MAC、风险标签、WIFI 分类、WIFI 所在位置、围栏内最后出现时间、关联设备数等。

3、设备同网扩线

系统具有批量导入设备四码信息进行同网扩线，根据输入的设备四码信息提取指定时间内输入设备的扩线 WIFI 信息，以及扩线 WIFI 下的其他同连或高频扫描设备信息。

扩线 WIFI 信息包括名称、MAC、风险标签、分类、所在位置、关联输入设备、扩线设备数量。

扩线 WIFI 所扩线出来的设备信息包括：设备 ID、机型、特征标签、常驻地、手机号归属地、最新位置、关联输入设备、关联扩线 WIFI 数。

4、WIFI 同网扩线

系统具有对 WIFI 进行深度同网扩线，通过批量导入 WIFI MAC 信息，提取这批 WIFI 下连接或高频扫描的设备信息，包括设备

ID、机型、特征标签、关联输入 WIFI 以及关联扩线 WIFI 数。在此基础上，系统还可以根据设备关联扩线的 WIFI 继续寻找该 WIFI 下同连或高频扫描的同网设备信息，展示设备 ID、特征标签、最新位置、关联输入 WIFI 以及关联扩线 WIFI 数等。

3.2.1.4.智能分析

针对目前案件研判线索多，线索分析难度大等问题，涉网新型行为分析系统推出智能分析功能，是将现有线索进行统一录入，通过对线索的智能分析与扩线，最终推荐出风险设备与风险窝点，并按照风险程度进行区分，支撑研判人员快速定位，节省研判时间。

1、线索导入

具有为案件创建智能分析任务，实现关联线索的导入，导入内容包括设备线索、WIFI/网关线索以及 IP 线索。

1) 设备线索：设备四码（PN、IMEI、IMSI、MAC）、OAID、IDFA、安卓 ID，每种线索可录入 20 条。

2) WIFI/网关线索：具有录入 WIFI MAC 与网关 MAC，每种线索可以录入 10 条。

3) IP 线索：具有手动录入或批量文件导入 IP 线索，包括 IP 地址与时间，可具有 10000 条线索的导入。

2、特征筛选

通过线索导入数据可以快速提取出关键设备，再根据设备的涉案特征可进一步获取精准涉案设备，涉案特征可从 APP 安装、地址到访、前科库命中、设备标签等维度进行提炼。

1) APP 安装：具有批量添加 APP 信息，包括 APP 名称与包名，也可通过上传 APK 的形式获取 APP 信息。若在没有 APK 信息的情况下，可通过涉网新型行为分析系统自身的 APP 库进行精准

与模糊搜索，为研判人员提供信息来源。

2) 地址到访：研判人员可通过对嫌疑设备可能出现的区域以及时间进行圈定，一是可以在境内选择省、市、区、县，境外选择国家；二是可以通过虚拟围栏的技术将可能出现的区域进行绘制，对到访过此区域内的设备进行筛选。

3) 前科库命中：是对历史案件的关联，可选择历史备案数据进行关联，对命中前科库的设备进行筛选。

4) 设备标签：可按照标签维度进行设备的筛选，根据案件研判涉及的内容与标签的关联关系，通过选定各维度标签对设备进行筛选，可按照分类以及等级进行标签的快速选择。

3、分析结果

智能分析结果是输出风险设备与风险窝点，并按照风险等级进行区分，分为高、中、低三级，分析结果具有一键导出。

1) 风险设备

风险设备按照命中的案件线索数、案件特征数、行为特征、异常轨迹以及疑似开发者、生活机等个进行区分，按照高风险、中风险、低风险三个等级进行设备的区分。每一级展示命中的设备基础信息、特征标签以及命中情况等。具有对命中设备的筛选。

命中设备以及关联特征通过图形化的方式展示，将高、中、低三级分别用红、黄、绿三色进行区分，通过拖拽可以快速查看不同设备与涉案特征之间的关联关系。

2) 风险窝点

风险窝点是根据风险设备的 WIFI/网关、工作地、居住地、最后位置分别计算形成聚集窝点，风险窝点在

风险窝点按照高风险、中风险、低风险三个等级进行分类，在地图上用红、黄、绿三种颜色进行区分。展示出风险窝点的详细地址、经纬度以及区域内风险设备的数量以及风险 WIFI/网关

的数量。

3.2.1.5.回流分析

目前大量电诈嫌疑人被移交回国，全国各地公安纷纷前往边境押解涉诈嫌疑人回乡，这批回流人员并未按照窝点以及类型进行分类，加上嫌疑人大多未携带工作/生活的手机等设备，所以只能采用审讯方式进行案研判，难度较大。针对此类情况，如何快速明确嫌疑人犯罪事实以及核实嫌疑人员涉案信息成为当前的工作难点，涉网新型分析系统具有通过回流人员手机号进行快速的分析以及定位其涉案性质的功能，助力对回流人员的研判，支撑我们审讯定罪。

系统具有通过回流人员提供的手机号可以找到关联设备的设备基础信息、境外停留天数、境外位置轨迹、命中境外园区以及特征标签等。通过设备境外轨迹情况可以获取境外聚集窝点情况，通过嫌疑设备的 WIFI 聚集情况以及风险标签，扩线出更多风险设备以及境外园区等。具有在地图上展示设备、园区、WIFI 等的地理位置信息。

3.2.1.6.APP 分析

系统具有对目标群体的提数结果展示、画像分析和窝点分析。

系统具有对分析结果的群体画像，可进一步通过特征标签、性别、年龄段、原籍地等维度进行筛查，对筛查结果进行画像分析。分析维度包括性别分布、年龄分布、群体特征标签、敏感 APP 安装情况、机型占比、手机语言占比、原籍地分布等维度。

针对作案人员，通常会在特定时段内聚集在作案窝点内，大量工作机连接同一工作 WiFi 的特点，因此可结合目标群体的位置分布和活动轨迹分析其聚集情况，针对涉案 APP 提取出的设备，

系统根据设备 LBS 位置、同连 WiFi 等情况，自动分析聚集人数 top5 的点位，作为可疑窝点，提供具体经纬度、WiFi 热点、聚集人员及人员画像等信息，在此基础上，研判人员可结合公安数据进行分析研判，锁定可疑的窝点位置及团伙成员。

3.2.1.7.IP 分析

实战中，公安机关利用现有手段可获取作案人员虚拟身份（微信、QQ 号等）及登录账号的 IP 地址，具有 IPV4 和 IPV6，包括固网 IP 和移动 IP，平台中可对 IP 地址可进行反向查询，查询特定时段内使用该 IP 的路由器设备、移动终端设备，提供路由器 MAC 地址、经纬度及移动终端设备的四码信息等，研判人员可据此锁定作案窝点、作案人员等。

同时，也可根据移动设备五码查询该设备特定时间段范围内 IP，进一步丰富研判分析线索。

3.2.1.8.WiFi 分析

平台内涵盖全球大量商用、民用 WiFi 热点数据，可通过 WiFi 路由 MAC 地址，筛选特定时段内的连接设备与扫描设备。实战中，在发现作案窝点的 WiFi 热点后，可通过检索该 WiFi 热点下历史连接设备，扩线团伙其它成员，但通常连接窝点 WiFi 的均为作案团伙使用的工作机，无法有效落地人员实名身份，因此，也可利用窝点 WiFi 热点下历史扫描数据，分析频繁出现但未连接，且曾在国内高危地出现过的设备，作为可疑的生活机，通常根据生活机号码可进行身份落地。

另外本功能可根据 WiFi 的 MAC 信息对指定 WiFi 生成一个月内该 WiFi 下人群特征画像。系统自动计算近一个月连接人数分布、近一月白天夜晚连接人数分布；分析该类人群的 APP 特征画

像，包括敏感 APP 安装情况、小众 APP 安装情况等；分析该类人群性别分布、年龄分布、人群特征标签；分析设备特征情况包括机型占比、手机语言占、原籍地分布、省份城市分布等。

3.2.1.9.群体分析

在部分案件中，我们通过前期侦查和扩线积累，可以获取一批作案人员的四码信息（手机号、MAC 地址、设备码、卡码）。获取到的信息可以通过群体分析，对设备信息匹配、画像分析、人群点位、聚集分析等。同时，通过系统的 APP 分析、IP 分析得到的群体数据，也可以导入到群体分析中做进一步的分析。

1、任务详情

群体分析任务具有以列表的形式展示用户创建的任务，包括任务名称、更新时间、任务描述、任务状态和任务查看等操作。任务分析状态包括计算中、任务完成、任务失败和新增数据暂未重算等。具有通过分析状态和更新时间对已有任务进行筛选查询。

任务具有详情查看、复制、重新计算、删除和刷新等操作，来对建立的任务进行管理。

2、任务创建

群体分析任务创建通过自定义任务名称、选择数据源、选择功能项、数据处理方式和添加描述等步骤完成创建。系统自动进行分析匹配对选择的群体进行按设置情况进行计算。

数据源选择上具有以文件的形式上传、批量添加和已有任务导入。当以文件形式上传时，可下载数据填写的模板文件，具有上传四码数据或四码中任意一码，数据总条数最多具有 50000 条，填写完成后具有一键拖入上传框进行上传；批量添加具有设备四码数据上传，最大具有 1000 条数据录入；已有任务导入时，具有 APP 分析和 IP 分析的任务，通过对应任务名称导入需要分析

的数据。

功能选择具有设备信息、人群定位、画像分析和聚集分析的自定义功能勾选。具有对设备信息进行匹配，展示目标人群设备的相关信息，包括：设备码、设备机型、基本信息、特征标签、最新位置、原籍地和常驻地位置信息；具有对人群进行定位分析，展示目标群人的位置信息，包括：最新位置、家庭地和工作地；具有对人群画像进行分析，展示目标人群的多维画像，包括：APP 特征画像、特征标签画像、性别年龄分布特征、机型信息分布特征和原籍地分布特征；具有对人群聚集地进行分析，展示目标人群潜在的聚集情况：可按照 WiFi、工作地、家庭地和最新位置进行分析，显示聚集分析报告和聚集设备信息。

数据处理具有多类数据源分析情形下，数据的合并处理或碰撞梳理。可在数据详情中对多类数据进行查看，包括数据源名称、上传方式、数据量、删除操作和总数据量。设备描述可对该任务添加自定义描述，方便研判人员备注信息。

3、条件筛选

群体分析结果具有条件筛选过滤，条件筛选包括快捷筛选和高级筛选。快捷筛选中通过选择包含条件或过滤条件，快速进行结果数据筛查。筛选条件包括设备特征、设备数据情况、APP 安装情况和数据来源情况。

设备特征具有对特征标签、原籍地、设备语言和其他特征筛选；设备数据情况具有对设备码非空条件进行筛选；APP 安装情况具有对 APP 分类和 APP 名称/包名进行筛选；数据来源具有对创建任务中的数据源进行筛选。高阶筛选中具有以并集或交集的形式对所有维度特征进行组合筛选。针对选择的筛选条件具有重置，确认筛选后可直接对分析结果按照设定的条件进行筛查。

4、设备信息

群体分析任务中系统自动计算群体匹配结果，分析结果或筛选结果具有以设备信息列表的形式进行展示。结果详情包括设备 ID、设备信息、特征标签、数据来源、最后停留位置、常驻地、原籍地、基础信息等。分析结果具有检索，检索维度包括 PN、IMEI、IMSI、MAC，并且检索条件具有重置。同时分析结果具有导出至 Excel，以利用其它手段进一步研判。

5、人群点位

系统具有对匹配出的设备信息点位进行可视化展示，输出其最新位置、家庭地和工作地的点位信息，不同类型点位以不同颜色进行标注，可辅助公安机关掌握所关注人群的最新位置及常驻地点。

点位数据在地图上具有聚合展示，放大后可查看该点对应的设备 ID、位置信息和经纬度信息，点位结果具有导出至 Excel。同时可通过设备 ID 检索关注目标，查看其在地图上的打点情况。

6、画像分析

针对群体分析匹配数据，系统具有对该群体进行画像特征分析，方便用户把控群体特点、发掘潜在特征、快速进行大量数据的研判分析。分析维度包括敏感 APP 安装特征情况、一般 APP 安装特征情况、特征标签情况、性别比例分布、年龄分布、机型设备占比 TOP10、手机语言占比 TOP5、原籍地分布、省份分布 TOP10、城市分布 TOP10。

系统利用大数据技术智能分析自然样本特征并与关注群体进行比较，提取差异化特征，将显著特征从强到弱进行排序。具有按敏感 APP 名称、敏感 APP 分类、一般 APP 名称、一般 APP 分类进行排序，同时具有将分析出的 APP 特征、类别或特征标签加入筛选条件，在全量结果中进行筛查。

7、APP 扩线

针对群体分析结果，系统能够智能分析出群体中各类 APP 的安装情况，包括一般 APP 和敏感 APP。用户可以通过 APP 类型和 APP 报名主动筛选群体安装的特定 APP。针对群体安装的 APP 情况，系统能够分析出该 APP 在群体中的安装总数、当前 APP 安装在群体中的占比、当前 APP 安装在自然样本的占比、APP 的小众程度、人群安装特征等。

用户可以将该 APP 加入筛选，进一步分析该群体中安装该类 APP 群体的特征，或者直接选择特定 APP 直接进行提数，分析安装该 APP 的群体特征，极大的方便用户通过群体分析的结果扩线出更多的可疑人员。

8、聚集分析

针对群体分析结果数据，系统具有对该群体进行聚集分析，生成每个聚集点的聚集分析报告，方便用户进行群体窝点研判。聚集分析报告包括基础信息报告和详细研判报告，展示了聚集点位置信息、经纬度和识别 ID 数量以及群体安装各类型敏感 APP 人数占比等信息。

聚集点识别中，具有按 WiFi 聚集、工作地聚集、家庭地聚集、最新位置聚集维度进行计算，计算结果数据具有以列表或地图的形式进行展示，当以列表形式进行展示时，还可选择查看辖区内聚集点、境内聚集点和疑似境外聚集点。当以地图形式展示时，具有地图打点展示并标记中文地址、经纬度信息和聚集人数数据。

当聚集点按 WiFi 连接情况分析识别时，具有展示聚集点地理位置、连接 WiFi 名称、WiFi MAC 地址、聚集人数、风险标签等信息。风险标签信息具有筛选，且具有选择多个风险标签，筛选结果同时满足所有条件。当聚集点按工作地、家庭地或最新位置分析识别时，具有展示聚集地址地理位置信息、聚集人数和安

装敏感 APP 占比。

聚集设备详情具有以列表的形式进行展现，包括设备 ID、设备信息、基础信息、特征标签、数据来源、安装敏感 APP 情况、原籍地信息、常驻地信息、最后停留位置等，具有将聚集点的设备进行导出至 Excel。

9、生成逻辑

系统具有对最终的分析结果进行生成逻辑查看，包括任务名称、任务描述、有效数据量、任务状态、创建时间、更新时间等。其中有效数据指已去除空数据、重复和错误数据后的结果。具有查看任务组成，即群体分析的数据来源情况以及不同数据源取合并或取碰撞的情况。

3.2.1.10.标签分析

系统具有根据标签模板提取符合特征标签的设备数据信息，或根据实际需求自主选择标签和标签组合进行提数，提取辖区内的设备数据。

该标签分析可以提取辖区内潜在网络传销相关的设备、疑似洗钱的设备、疑似杀洋盘的设备、潜在黑灰产设备及潜在网赌设备等，主动根据设备标签发现辖区内风险设备。

3.2.1.11.APK 解析

系统具有 APP APK 解析，对用户上传 APP 的 APK 安装包进行解析，解析获得注册信息、域名、SDK 和源代码信息。

包含基本信息、域名分析、SDK 分析和源代码分析。

3.2.1.12.人群点位

系统可通过输入人员 ID 的方式，具有最多对 500 个人员进行分析，输出其最新位置、家庭地和工作地等信息。可辅助我们掌握所关注人群的最新位置及常驻地点。

3.2.2.预警阻断

系统具有结合互联网大数据建模能力，汇总案源应用和主动发现应用信息，实时获取辖区内潜在受害人群及易受骗人群，潜在受害人是安装了某款涉案应用结合用户画像建模计算的群体，易受骗人群是根据安装可疑应用结合用户画像建模计算的群体的功能。

3.2.2.1.预警统计中心

预警统计中心是以大屏的形式展现与本地相关的预警数据统计及分析情况。能够依据本地实际情况分别查看今日、昨日、前 7 日、前 30 日、前 3 月、前 6 月、前 1 年的预警统计情况。

具有分别展示选中时间段内本地的预警统计情况，也能够以地图的方式按照不同的辖区分别展示选中时间段内的预警人数。

具有实时展示推送的预警消息，展示内容包括：手机号、预警来源、预警类型、易受骗分、预警区域、最新预警时间以及处理情况。

具有以折线图的方式展示预警人数趋势变化情况，以及劝阻人数的变化情况。能够以柱形图的方式展现各类型诈骗的预警类型分布，以蜘蛛网图的形式分析预警来源分布情况。

能够统计各辖区的回访处理情况，统计维度包括：已接听电话数、已宣传人数、本地人数、劝阻金额、被骗次数、以及被骗

金额等，同时能够分析出总的被骗金额以及劝阻金额。

具有对预警卸载量进行分析统计，能够将辖区内预警后的 7 日卸载率与自然样本进行比较，直观反应本地的预警效果。7 日卸载率为预警消息产生后，已卸载高风险 APP 人数占总预警人数比例， $7 \text{ 日卸载率} = \frac{\text{卸载时间} - \text{预警时间}}{\text{总人数}} \times 100\%$ 。统计周期为 7 日，例如 15 号统计的为 1-7 号期间预警总人数卸载情况。

具有对各类型的诈骗 APP 卸载量进行分析，统计出不同类型的 7 日卸载率，并与自然样本进行比较，以及与上月的情况进行比较，能够帮助公安机关直观了解各类型诈骗预警的效果，方便采取更进一步的行动。

3.2.2.2.预警应用管理

预警应用管理模块具有展示来源于报案信息、用户导入和云脉发现三个途径的预警应用。公安机关根据实际情况，可对预警应用范围进行自主设置，可设置预警应用来源和诈骗类型。还可针对无需预警的应用设置白名单。

3.2.2.3.预警数据导入

系统具有第三方的预警数据导入预警阻断平台进行统一的预警消息下发及回访工作。当前系统具有导入的预警消息来源包括：部平台下发、4G 分光预警、qq\微信预警、运营商预警以及其他第三方平台的预警数据等。导入预警数据时需选择易受骗分，易受骗分代表本批导入人群的易受骗程度，默认 60 分。可根据预警来源判断并修改。当易受骗分小于 100 为低风险，100-149 为中低风险，150-199 为中风险，200 以上为高风险。

导入数据按照模版样式进行导入，具有下载模版，导入文件

大小限制 5M 以内，单次最多上传 20000 条数据。填写好模版后能够直接上传到系统进行统一的预警消息推送。

系统具有对已导入的数据进行查询和统计分析，查询条件包括：导入时间、预警来源、下发状态等。统计分析的维度包括：手机号码、诈骗类型、预警来源、易受骗分、导入时间、下发状态、下发时间等，并且能够进行一键导出之前导入的预警数据。

3.2.2.4.潜在受害人管理

系统能够主动推送辖区内的潜在受害人，通过对潜在受害人安装和使用可疑涉诈 APP 的情况，以及用户画像等多维度特征，计算得到易受骗分，并以列表方式推送潜在受害人详情。易受骗分范围为：0-300。当易受骗分小于 100 为低风险，100-149 为中低风险，150-199 为中风险，200 以上为高风险。

系统通过建模计算潜在受害人，并推送相关数据，包含手机号码、号码置信度、预警来源、诈骗类型、安装应用、易受骗分、常驻地等人员信息。具有查看人员标签，及预警处理记录。当有人新安装可疑 APP 时，系统及时给出预警。该类人员可能为潜在的受害人员，通过潜在受害人的及时发现，辅助我们进行预警阻断。

3.2.2.5.易受骗人群管理

系统能够主动推送辖区内的易受骗人群，通过对易受骗人群安装和使用可疑敏感 APP 的情况，以及用户画像等多维度特征，计算得到易受骗分。

易受骗人群管理模块展示系统建模计算的易受骗人群，包含手机号码、号码置信度、其他 ID、易受骗类型、易受骗分、安装 APP 总数、安装特征 APP 情况、家庭地、工作地、最新位置、

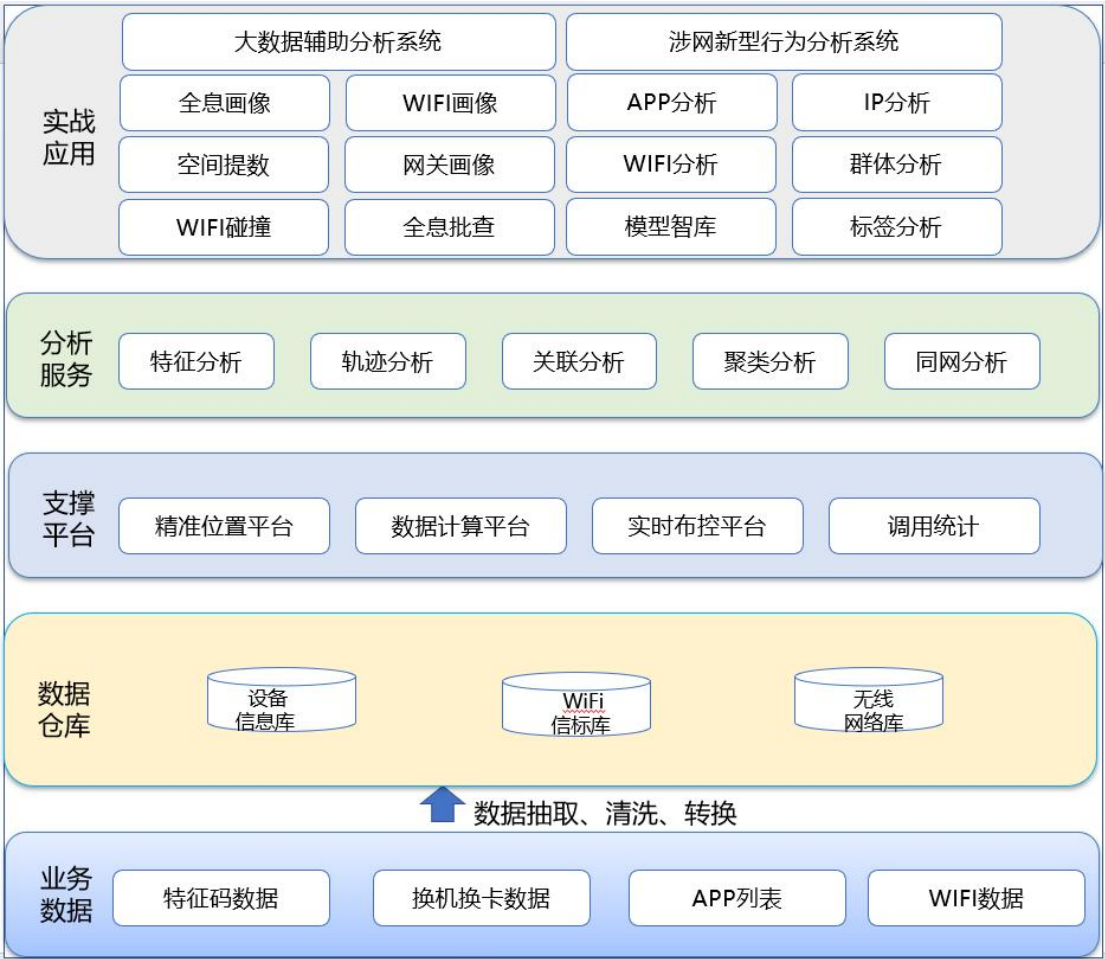
预警时间等人员信息。当辖区内有系统模型发现的易受骗人群时，系统及时给出预警。该类人员可能为易受骗人员，通过潜在易受骗的及时发现，辅助公安机关进行预警预防工作。

第四章 项目设计方案

4.1.总体架构及技术路线

4.1.1.总体架构

系统总体架构图如下：



4.1.2.技术路线

本项目采用的核心技术包括：Hadoop 分布式存储和计算、Spark 大规模数据处理引擎、Tensorflow 深度学习平台和 Kubernetes 容器化调度平台等。

4.1.2.1.Hadoop 分布式存储和计算平台

本项目中，涉及多类移动互联网数据的存储、计算，数据量非常庞大，为了实现海量大数据的分布式存储和计算，采用 Hadoop 分布式存储和计算平台。Hadoop 是一个分布式系统基础架构，由 Apache 基金会开发，用于开发和运行处理大规模数据。Hadoop 平台使用户可以在不了解分布式底层细节的情况下，开发分布式程序。充分利用集群的威力高速运算和存储，Hadoop 主要有以下几个优点：

高可靠性：Hadoop 按位存储和处理数据的能力值得信赖。

高扩展性：Hadoop 是在可用的计算机集簇间分配数据并完成计算任务的，这些集簇可以方便地扩展到数以千计的节点中。

高效性：Hadoop 能够在节点之间动态地移动数据，并保证各个节点的动态平衡，因此处理速度非常快。

高容错性：Hadoop 能够自动保存数据的多个副本，并且能够自动将失败的任务重新分配。

低成本：与一体机、商用数据仓库以及 QlikView、Yonghong Z-Suite 等数据集市相比，hadoop 是开源的，项目的软件成本因此会大大降低。

Hadoop 由许多元素构成，包括分布式文件系统 HDFS、MapReduce 处理过程，以及数据仓库工具 Hive 和分布式数据库 Hbase 等。

4.1.2.2.YARN 资源调度平台

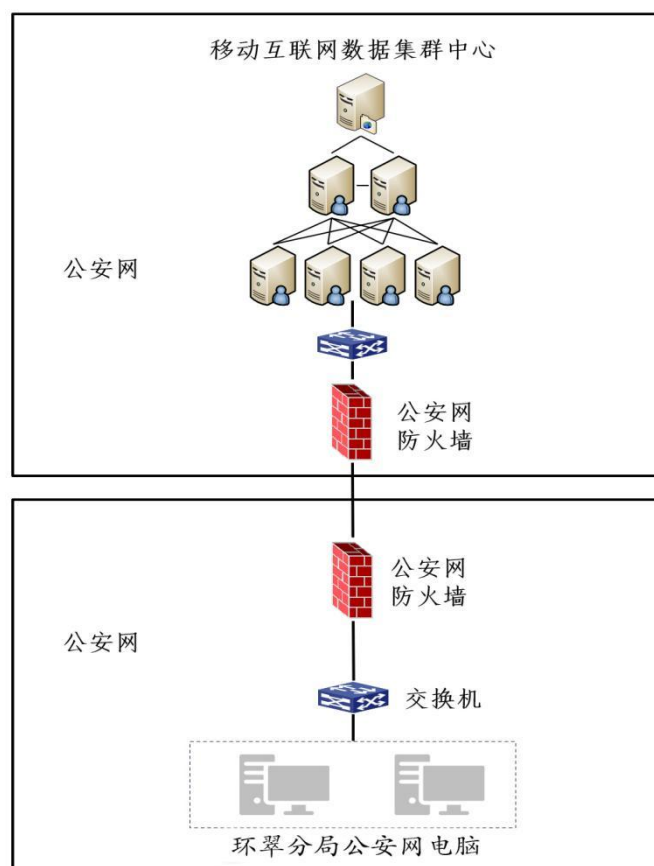
YARN 是一个资源管理和任务调度的平台，用来对 Hadoop 集群的存储和计算资源进行统一管理和调度，使得各种类型的应用运行在 Hadoop 上面，并通过 Yarn 从系统层面进行统一的管理。有了 Yarn，各种应用就可以互不干扰的运行在同一个 Hadoop 系统中，共享整个集群资源。

4.1.2.3.Spark 大规模数据处理引擎

在大数据的处理和机器学习过程中，需要高速的数据处理性能和数据迭代计算能力，Spark 是基于内存计算的大数据并行计算框架，基于内存计算，提高了在大数据环境下数据处理的实时性，同时保证了高容错性和高可伸缩性，允许用户将 Spark 部署在大量廉价硬件之上，形成集群。

4.2.系统拓扑图

系统拓扑图如下：



采用在公安网提供大数据辅助分析查询系统和涉网新型行为分析系统服务的方式，分局公安网电脑可通过数字证书登录访问并使用。

4.3.网络系统设计

项目整体网络都在公安网内，不涉及数据的跨网传输。

4.4.安全系统设计

信息系统具有系统开放性、资源共享性、介质存储高密性、数据互访性、信息聚生性、保密困难性、介质剩磁效应性、电磁泄露性、通信网络的脆弱性等特性，这些特性对信息系统的安全构成了潜在的危险。本项目的安全需求包括以下几方面：

4.4.1.网络层安全

网络层的安全风险主要包括重要数据的泄露与篡改，以及来自其他网络的安全威胁。数据泄露与篡改的安全威胁主要是网络数据传输线路之间存在被窃听和攻击的隐患。一方面网络存在遭受内部攻击的可能，敏感信息可能被来自内部的侵袭者窃取和篡改；另一方面本系统建成后将从社会各部门，甚至是互联网获取相关的信息，也存在外部攻击的安全隐患。本项目网络安全需求如下：

访问控制：由防火墙将内部网络与外部不可信任的网络隔离，对与外部网络交换数据的内部网络及其主机、所交换的数据进行严格的访问控制。对内部网络使用防火墙将不同的 LAN 或网段进行隔离，并实现相互的访问控制；

数据加密：在数据传输、存储过程中防止非法窃取、篡改信息的有效手段；

安全审计：识别与防止网络攻击行为、追查网络泄密行为的重要措施之一。一是采用网络监控与入侵防范系统，识别网络各种违规操作与攻击行为，即时响应（如报警）并进行阻断；二是对信息内容的审计，可防止内部机密或敏感信息的非法泄漏。

4.4.2.系统层安全

系统级的安全隐患主要针对本项目拟建系统采用的操作系统、数据库及相关商用产品的安全漏洞和病毒威胁。

对于系统的安全防范采取如下策略：

尽量采用安全性较高的网络操作系统并进行必要的安全配置

关闭一些起不常用却存在安全隐患的应用

加强口令字的使用（增加口令复杂程度、不要使用与用户身份有关的、容易猜测的信息作为口令）

及时给系统打补丁

系统内部的相互调用不对外公开

严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

充分利用操作系统本身的日志功能，对用户所访问的信息做记录，为事后审查提供依据。

4.4.3.应用层安全

应用层的安全隐患主要包括应用软件以及应用终端的身份认证漏洞和非授权访问。

接入平台内所有的终端设备都应满足国家或公安行业相关的技术标准和要求，具备国家相应权威部门出具的产品证书和安全检测报告，并在检测报告允许的范围内使用，关键安全设备必须接受监管系统的监管和审计。终端安全主要体现在如下几个方面：终端设备认证、终端访问控制、传输保护。

身份认证包括如下几点：

对登录系统的民警的身份认证，一般采用 PKI 身份认证方式，对于部分安全级别特别高的功能，还需要通过指纹进行认证。

终端设备识别：客户端收集终端硬件信息，并提交给网关，网关根据终端软硬件特征确保只有经过注册的合法终端才能与平台连接，保证终端设备的合法性。

终端访问控制：在终端与平台完成连接认证时，通过设置细粒度访问控制策略，确保非法用户不能访问，合法用户不能越权访问。

传输保护：终端客户端与网关之间使用 SSL 协议对通信过程

进行加密和完整性保护，保证数据传输的安全性。

4.4.4.数据层安全

数据层的安全隐患主要是指数据的集中存储造成数据容灾性差，可能因突发事件造成数据的不可恢复丢失。数据层的安全设计如下：

通过增强加密技术、密钥管理、数据隔离、数据多备等手段，保证数据安全。包括数据存储安全、数据传输安全、数据安全备份等。

数据存储安全：对数据自身进行加密，防止由于硬盘被盗、笔记本电脑丢失、存储介质丢弃等造成重要数据泄密的可能性发生。

数据传输安全：在数据传输过程中采用加密手段，利用国家批准使用的密码算法对数据加密，保证数据安全。在涉密网络及非涉密网络之间使用安全可靠的数据交换方式。

数据安全备份：采取先进的数据存储和备份技术及设备保障信息的存储安全。

4.5.终端系统及接口设计

无。

4.6.其它系统设计

无。

4.7.信息资源规划及项目形成的信息资源目录

无。

4.8.云服务需求或系统软硬件配置及部署方案

项目建设采用购买 SaaS 系统服务方式，不涉及本地云服务以及软硬件配置，无需本地部署。

第五章 项目组织管理

5.1.项目组织机构

1、项目领导小组：

组长由分局分管领导担任

成员包括：警务合成作战大队、刑侦大队负责人。

项目领导小组职责如下：按照项目建设合同，审核批准项目实施计划，负责数据资源的接入协调，根据项目过程中的进度、质量、技术、资源、风险等实施宏观监控。

2、项目负责人

由警务合成作战大队一名民警具体负责

职责：全面负责项目的实施工作，根据项目要求制定项目实施计划，项目进度监督，配合和协助乙方做好协调工作。

3、技术支持组

由系统建设厂家负责整个项目的技术支持工作。

职责：按照项目领导小组和项目负责人的总体要求系统进行安装调试，试运行、交付，对使用人员进行技术培训。

5.2.项目进度安排

服务期限为一年，签完合同后进入一年的正式服务期，一年内完成项目的交付、培训、终验等服务。

5.3.安全管理制度

1、针对平台制定信息安全工作的总体方针和安全策略，并说明机构安全工作的总体目标、范围、原则和安全框架等信息。对安全管理活动中的各类管理内容建立安全管理制度。

2、指定或授权专门的部门或人员负责安全管理制度的制定；安全管理制度具有统一的格式，并进行版本控制；组织相关人员对制定的安全管理制度进行论证和审定，并通过正式、有效的方式发布；安全管理制度应注明发布范围，并对收发文进行登记。

3、信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定。定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。

5.4.人员培训

拥有一支技术过硬的系统使用队伍，成功实现技术的转移是保证系统顺利建设并长期稳定、良好运转的重要保障。需对相关人员进行技术培训，在以后系统运行过程中亦需根据系统应用的深入进行相应内容的培训，以保证系统的管理人员和应用人员能够及时、准确的了解和熟练使用系统。

1、培训对象

针对拟使用本系统的分局民警

2、培训方式

根据培训内容的实现方式，可分为现场安装培训和授课培训。

1) 现场培训

现场培训是在现场进行使用培训，相关使用人员在现场观看和学习，并给予实际操作机会，技术培训人员针对本系统的特点和应用系统维护要求作相应的讲解，对相关使用人员产生的问题随即解答并直到相关人员学会为止，具有很强的实践和交互性，但人数不能过多。这种方式的培训在所有设备的安装和调试中都将积极予以实现。

2) 授课培训

授课培训一般提供较为系统的理论学习，并根据不同课程辅以实验环境下的实际操作，学习过程中还提供完备的学习资料，是正规培训主要采用的方式。

3、培训内容

为保证项目顺利实施、平台正常运行、后续应用推广，相关人员必须进行专业的培训。

5.5.保障措施

供应商服务内容必须包括：不限定时间电话技术服务、现场开发技术服务、远程故障排除、定期巡查服务、技术升级服务、接口服务、相关规范标准变更后的修改服务等。

具体的服务内容包括：

(1) 不限定时间电话技术服务

供应商将提供多个技术服务点的固定服务电话和主要技术服务人员的手机号码，提供 7*24 小时的电话服务。

(2) 现场开发技术服务

根据用户的需要提供用户现场开发的技术服务。

（3）远程故障排除

通过公安网、电话、视频等方法，可以在远程对系统故障进行诊断和及时排除服务。

（4）定期巡查服务

供应商将提供每三个月一遍的巡查服务，及时跟踪各地的系统使用情况，发现系统运行故障。

（5）技术升级服务

供应商将在合同规定时间内免费提供平台在保修内功能扩充和升级服务，安装最新版本的程序并提供全套的系统升级相关的设计开发及维护资料。

（6）相关规范或标准变更的修改服务

根据确认后的规范或标准变更要求，提供系统相关的数据或程序变更的修改服务。

第六章 项目投资

6.1.项目资金预算

本项目提供的大数据辅助分析查询系统服务和涉网新型行为分析系统服务，不涉及硬件建设与软件开发，项目建设预算为600000元，服务期限1年。在服务期限内，如查询次数超出清单中最大服务次数，供应商应当免费增加查询服务次数，不再收取任何费用；如查询次数少于清单中最大服务次数，供应商应当

适当增加服务期限。清单如下：

序号	功能模块			详细描述	许可数	最大服务	价格
					(个)	次数	(元)
1	大数据辅助分析查询系统	全息画像	特征码信息	通过对方提供的设备数据，查询其相关数据分析结果。	2	30,000	270000
			画像推测	大数据画像，对设备打标签。	2	30,000	
			线上行为	分析设备安装的 APP 列表，并进行分类提示。	2	30,000	
			常连 WiFi	分析近段时间特定设备的常连 WiFi。	2	30,000	
			关系图谱	分析目标数据信息的关系图谱，寻找目标数据之间的相互关系。	2	30,000	
			历史 IP	展示设备关联的历史 IP 信息。	2	30,000	
			点位管理	分析和实现点位回溯功能。	2	30,000	
			点位分析	分析设备近期点位。	2	30,000	
			关联基站	通过对目标设备的关联基站进行查询，可查看设备连接的基站和连接时间。	2	30,000	
		WiFi 画像		▲对指定 WiFi 设备进行查询筛选。	2	10,000	
		基站画像		根据基站信息查询基站画像，包含基站位置分布与基站热力图。	2	1,000	
		网关画像		支持查询网关设备下关联的网络环境、设备等信息。	2	1,000	
		空间提数	基站提数	对指定基站设备进行查询筛选。	2	10,000	
			围栏提数	对指定时间段围栏下的设备进行筛选。	2	100	
		智能研判	WiFi 碰撞	通过多个目标 WiFi 的碰撞，分析出关联的设备情况。	2	500	
			全息批查	▲支持批量查询设备信息，查询其相关数据分析结果。	2	100 次（任务数）	

2	涉网 新型 行为 分析 系统	打击 反制	应用管理	管理风险应用，分析应用趋势和同源应用情况	2	无限制	330000
			模型智库	通过大数据建模分析发现风险网络环境及设备	2	3,000	
			资金流预警分类	对资金流预警对象进行类型识别与区分	2	3,000	
			境外围栏提数	对境外指定时间段围栏在的设备进行筛选	2	100	
			设备同网扩线	对批量导入的设备特征码信息扩线 WIFI 以及其他设备信息	2	3,000	
			WIFI 同网扩线	对输入的 WIFI 信息提取设备以及扩线出来的其他 WIFI 下同网设备信息	2	3,000	
			智能分析	多种线索整合分析，输出风险设备与窝点	2	3,000	
			回流分析	针对境外回流嫌疑人进行过快速研判以及线索挖掘	2	3,000	
			APP 分析	▲对安装指定 APP 的设备进行查询筛选并分析画像	2	3,000	
			IP 分析	▲对指定 IP 下的设备进行查询筛选并分析其关联网络环境	2	3,000	
			WiFi 分析	对指定 WiFi 下的设备及周边网络环境进行查询筛选及画像分析	2	3,000	
			群体分析	对指定若干设备进行设备信息分析、群体画像分析及点位分析	2	3,000	
			标签分析	对指定标签下的设备进行查询筛选和画像分析	2	3,000	
			APK 解析	对指定 APK 进行解析得出解析报告	2	3,000	
			人群点位	基于设备特征码进行群体设备点位分析	2	3,000	
		预警 阻断	预警统计中心	展现与本地相关的预警数据统计及分析情况	2	无限制	
			预警应用管理	对多方面来源的预警应用信息进行管理	2	无限制	
			预警数据导入	支持导入其他平台的预警数据	2	无限制	

			潜在受害人管理	推送潜在受害人设备详情	2	无限制	
			易受骗人群管理	推送易受骗群体设备详情	2	无限制	
			话务员管理	建立话务员回访体系，开通派出所话务员账号	2	无限制	
			话术模板管理	提供预警话术模版，支持自定义	2	无限制	
项目建设资金总预算（元）：							600000

6.2.项目资金来源和资金安排计划

本项目资金来源为区财政拨款，项目资金用于购买大数据辅助分析查询系统和涉网新型行为分析系统服务，服务期限为 1 年。