
全景分析系统建设方案

编制单位：威海市公安局环翠分局

编制时间：2024 年 7 月

目录

一、项目背景及必要性	3
二、现状和需求分析	3
三、项目建设内容	3
四、项目设计方案	3
4.1 总体逻辑架构及技术路线	3
4.2 系统拓扑图	4
4.3 应用系统设计	4
4.4 网络系统设计	5
4.5 安全系统设计	6
4.5.1 信息系统及网络安全性	6
4.5.2 数据安全性	7
4.6 终端系统设计	7
4.7 其他系统设计	8
4.8 信息资源规划及项目形成的信息资源目录	8
4.9 系统软硬件配置及部署方案	9
五、项目组织管理	9
5.1 项目组织机构	9
5.2 项目进度安排	9
5.3 安全管理制度	9
5.4 人员培训	10
5.5 保障措施	11
六、项目投资	12
6.1 项目资金预算	12
6.2 资金来源与落实	13

一、项目背景及必要性

略。

二、现状和需求分析

略。

三、项目建设内容

基于办案业务的现状及业务需求，需求补充覆盖全网的移动设备信息数据能力及金融类数据能力，但采用自建大数据平台接入这些数据进行应用方案，项目建设的技术难度大，建设周期长，资金投入多。通过市场调研后发现目前市场上有提供基本满足业务需求的数据技术服务的 SaaS 系统。采购 SaaS 系统技术难度低，由厂商提供所有现成的技术服务；建设周期短，直接申请即可开通账号使用系统；资金投入少。

SaaS 系统具有的贴近业务实战的主要功能包括：

（1）全息档案：包括针对手机设备、APP、WIFI 设备、IP 地址、实人档案（包括虚实转换及消费支付明细）相关信息查询能力。

（2）研判工具：包括圈选区域范围内的手机设备信息，圈选区域范围内的 WIFI 设备信息，提交 APK 文件进行解析。

（3）自主建模：包括建模筛选安装多个指定 APP 的移动设备信息，建模筛查关联多个指定 WIFI 的移动设备信息，建模筛查关联多个指定位置的移动设备信息，建模筛查关联多个指定位置和安装 APP 的移动设备信息。

（4）重点布控：包括针对移动设备信息更新的布控，针对 WIFI 设备信息更新的布控；针对 IP 信息更新的布控。

随着社会的进步、技术的发展，电信诈骗犯罪分子不断演化犯罪手段，我们也需要采用新的技术和理念，和行业领先的供应商一起建立密切的警企合作，一起打击电信诈骗犯罪。

四、项目设计方案

4.1 总体逻辑架构及技术路线

总体逻辑架构图如下



4.2 系统拓扑图

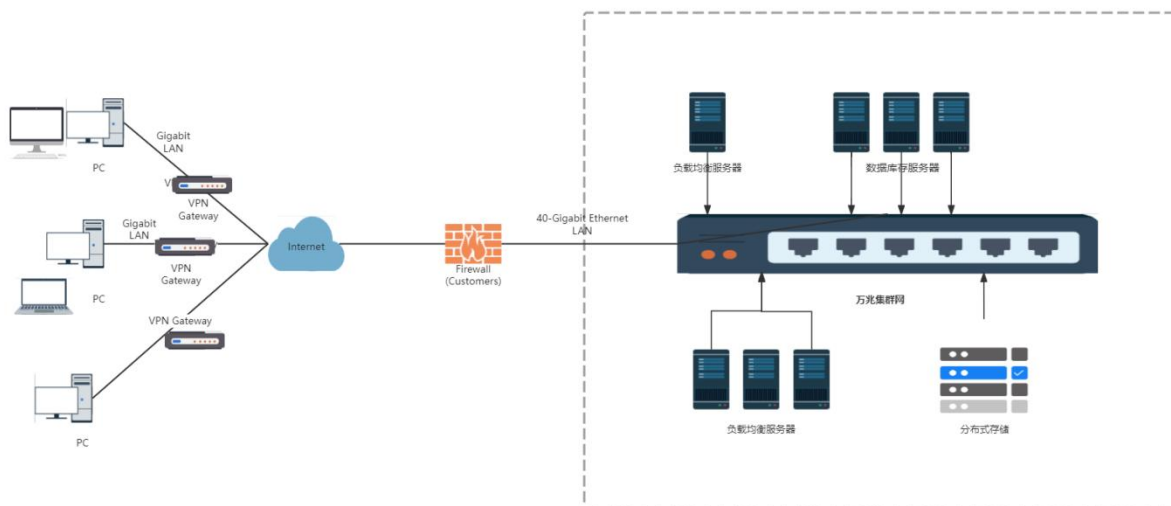


图-系统拓扑图

全景云开查询系统整体系统拓扑图如上设计所示，系统部署与服务提供商互联网本地服务器。我局系统工作人员需要通过 VPN 链接到服务提供商的本地服务器，然后发送数据查询、下载、搜索请求。服务提供商建立分布式存储服务器集群、数据库服务器集群、应用服务器集群。通过数据请求将数据库内对应的请求数据响应给我局，对于工具应用型请求，服务提供商应用服务器也能快速、及时响应，从而满足业务请求的需要。

4.3 应用系统设计

全景云开分析服务系统以微服务为基础架构平台，其逻辑架构分为 4 层。具体分为数据接入层、数据处理层、数据服务层以及业务应用层，具有水平及垂直扩展，保证整体的稳定性及扩充的弹性，

接入层提供多种数据接入方式，保障外部数据的无缝对接。

- (1) 数据接入层：数据接入层具有接入自有数据、第三方合作数据、企业一方数据及其他互联网数据；同时具有接入其他业务应用数据。
- (2) 数据处理层：根据平台架构设计，选择 HDFS、HBASE 存储接入层数据，通过数据挖掘、分析，利用数据建模、机器学习，从而构成各种模型库，再利用 Hive、Spark 处理计算。
- (3) 数据服务层：针对数据处理层的数据做相关的查询、挖掘、识别、研判、分析等服务，从而为业务系统层提供数据服务。
- (4) 业务系统层：包含实人档案查询、设备档案查询、网络反查、APP 列表挖掘、研判工具、自主建模等业务应用，通过 MySQL、elasticsearch 接口调用数据服务层的数据应用。

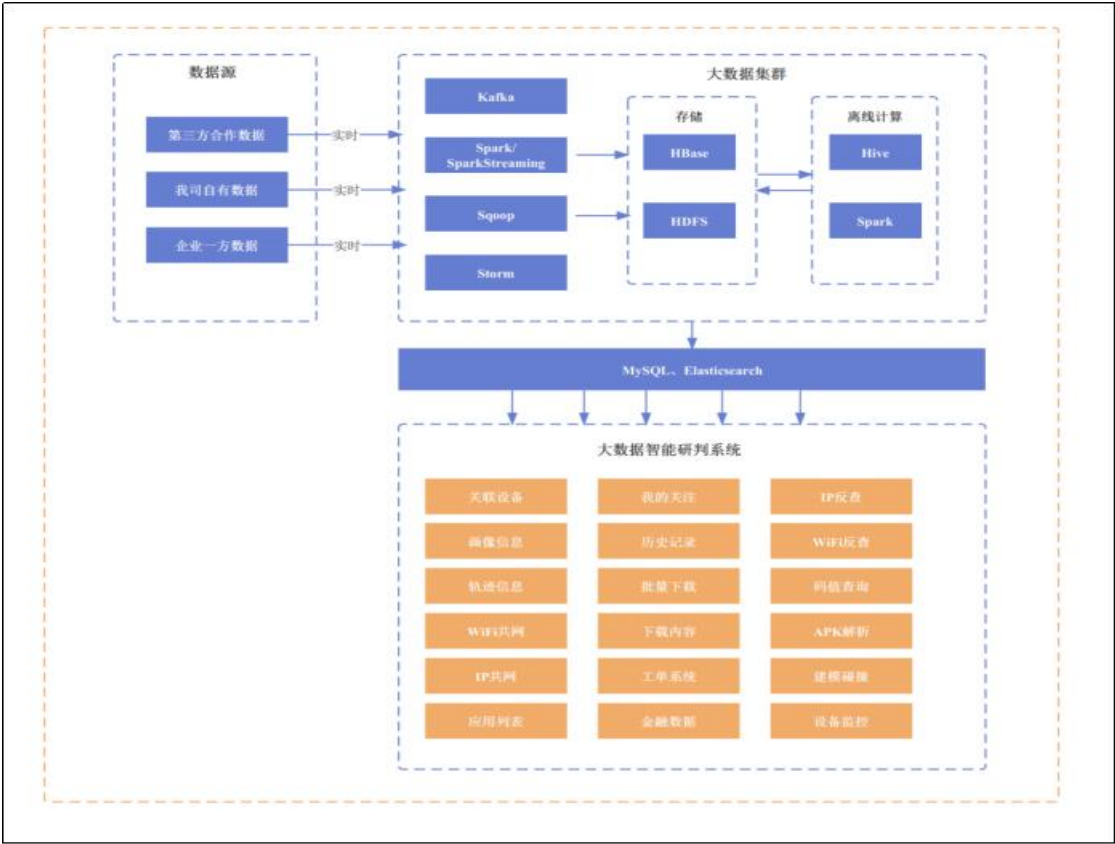


图-应用系统设计图

4.4 网络系统设计

硬件设备物理部署设计，对整个系统的网络结构、网络选型、网络应用均要按照先进性、成熟性、可靠性、开放性、安全性原则进行设计。在软件部署上采用系统内部署多套协同办公管理软件的分布式交换原则。该方案遵循以下原则和方法：

独立性：各功能模块分别部署，分别具有各自独立的服务器、网络及应用系统；根据各自的管理体系进行架构，公安机关对于每个功能模块的业务需求量相差较大到时候，系统运算可以相对独

立，从而保障业务的稳定性；

分布式交换：系统内部能够通过服务器进行数据之间的交换，分局与之间的数据能够通过专用的文件加密传输交换系统进行交流；

最小授权：本系统中仅对提供账号的公安用户进行独立的授权管理；没授权的账号是无法访问登录系统的。

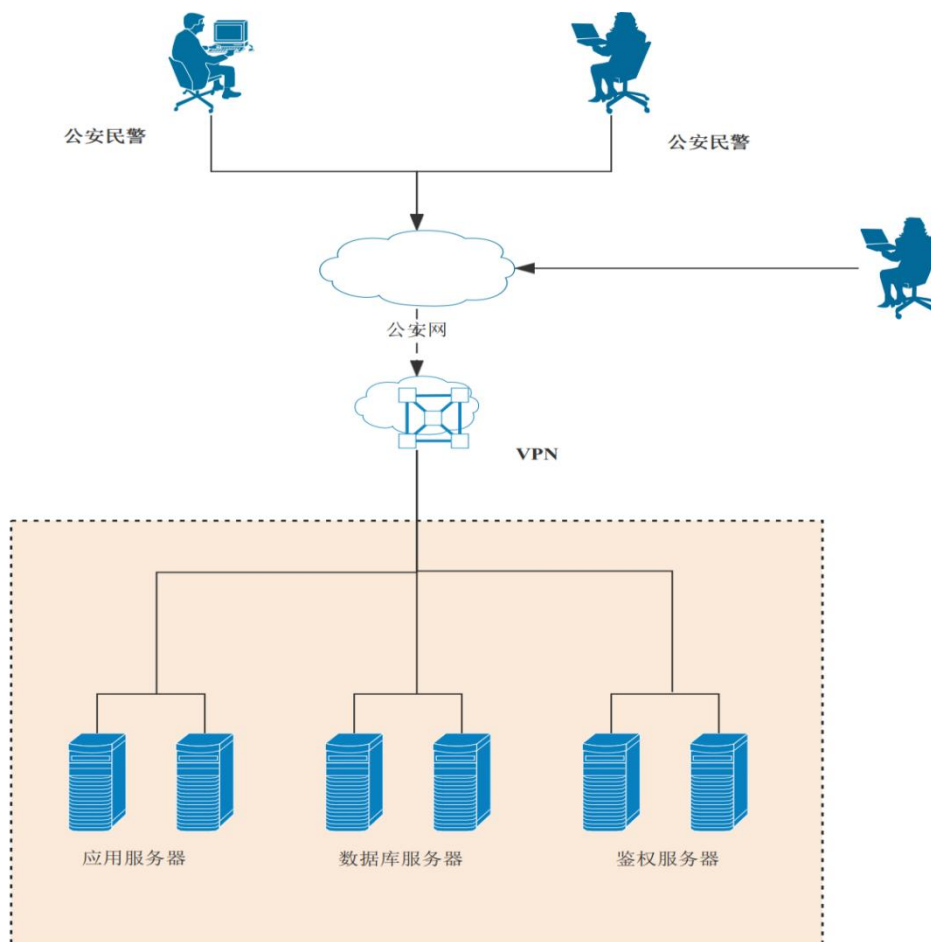


图-网络系统设计图

4.5 安全系统设计

4.5.1 信息系统及网络安全性

(1) 信息系统安全性：产品供应商系统所处网络环境需具备《信息系统安全等级保护 - 三级》备案证明；

(2) 网络交互安全性：为方便多场景使用，需具有互联网配合安全通道（VPN）技术访问产品

系统;

(3) 身份验证安全性: 每次登陆都需注册者手机号+验证码登陆;

4.5.2 数据安全性

(1) 数据隔离控制: 我局系统用户登陆、查询、下载等相关记录和数据确保与其他用户数据隔离;

(2) 用户权限控制: 根据注册的用户进行权限隔离控制, 用户账号间无数据共享、权限共享等设置;

4.6 终端系统设计

(1) 多码查询

要求具有通过目标设备的六码(手机号、IMEI、MAC、IMSI、idfa、oaid)数据其中一个特征码, 查询其对应的设备。

(2) 设备信息

要求具有展示目标人员的设备型号、厂商、设备语言、系统版本等信息。

(3) 画像分析

要求具有根据手机特征码查询目标人员的用户画像标签, 如性别、年龄、手机号、常驻地、居住地等人员身份标签。

(4) 码值信息

要求具有展示设备上关联的 Imei、OAID、Mac 信息, 以及设备上全部获取到的手机号和 IMSI 码值及其获取时段。

(5) 轨迹信息

要求具有展示目标设备近期活动轨迹, 并基于轨迹进行常驻地、居住地、工作地等分析。

(6) 常连 WiFi

要求具有分析目标移动设备 top20 常连无线网络设备及网络地址信息。

(7) WiFi/IP 同网关系人

要求具有根据设备与 WiFi 的关系, 分析目标设备的 WiFi/ip 同网关系人。

(8) 应用分析

要求具有展示目标设备上的 APP 安装、活跃、卸载行为, 并对应用进行分类提示, 可快速判断是否为重点关注对象。

(9) WiFi 档案

要求具有对指定 WiFi 下的设备进行分析、筛选、查询、提数。

(10) IP 档案

要求具有对指定 IP 下的设备进行分析、筛选、查询、提数。

(11) APP 档案

要求具有对指定 APP 下的设备进行筛选、查询、提数；并分析目标应用在境内境外的安装情况以及首装人群。

(12) 实人档案

要求具有身份证号、手机号和银行卡号的三要素互译，要求具有查询线下消费和云闪付转账信息，以及 YL 全流水交易数据。

(13) 地理围栏

要求具有通过在地图上选择指定区域对其进行布控，从而获得布控时间范围内出现在此区域内的设备信息。

(14) WiFi 围栏

要求具有通过在地图上选择指定区域对其进行布控，从而获得布控时间范围内出现在此区域内的 WiFi 设备。

(15) APK 解析

要求具有通过上传 APK 文件，分析其风险 URL、APP 信息、获取权限等内容。

(16) 自主建模

要求具有输出同时安装 3 款应用的移动设备；要求具有输出在指定时段内连接不同无线网络设备的相同移动设备；要求具有获取在指定时间内，出现在不同区域的相同移动设备；要求具有获取在指定时间内，出现在特定区域且有关应用安装在的移动设备；要求具有获取在指定时间内，连接 2 个及以上风险 IP 的移动设备。

(17) 重点布控

要求具有关注移动设备是否到访关注区域、是否连接指定无线网络设备、是否安装特定应用等行为；要求具有追踪无线网络设备是否与指定移动设备产生连接；要求具有追踪网络地址是否与指定移动设备产生连接。

4.7 其他系统设计

该项目为采购 SaaS 系统服务，不用部署在本地环境，不与本地系统进行对接、融合，不涉及应用支撑平台和应用系统建设。

4.8 信息资源规划及项目形成的信息资源目录

该项目为采购 SaaS 系统服务，数据不落本地库，不涉及信息资源规划和数据库建设。

4.9 系统软硬件配置及部署方案

该项目为采购 SaaS 系统服务，不用部署在本地环境，但需提供可连互联网的普通办公电脑，并安装谷歌浏览器用于登录 SaaS 系统。

五、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、网安大队负责人。

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

完善并加强业务安全管理，针对应用与服务各环节提出符合我局规范的管理制度和实施办法等。

需要逐步建立和完善的主要安全管理制度有：

（1）制订安全管理办法：明确安全目标和安全策略，各类数据资源的安全保护等级、管理要求。

（2）组织分工和责任，岗位职责、权限，电子政务系统评估、维护要求等。

(3) 制订应急响应制度：明确系统在异常和紧急情况下的应急组织、处理流程、要求等。

(4) 制订证件管理办法：明确数字证书、身份卡等各类证件的发放、使用、回收等的管理办法。

(5) 制订软件管理办法：明确操作系统、数据库、应用系统等软件的安装、更新、要求等管理办法。

(6) 建立安全审计制度：明确各类日志的备份要求、保存时间和安全审计周期、结果处理等的管理办法。

5.4 人员培训

分局工作人员获得软件使用授权后，开始系统使用培训。系统培训建议采用集中方式进行，分局制定培训考核办法，确保各参训人员能够切实理解系统的操作方式方法。培训时间一天。供应商提供在线咨询。

表：培训需求表

序号	名称	提供的资料	持续时间	培训对象	培训地点
1	系统培训	系统功能概述及维护	不少于 1 天	管理人员及使用人员	线上
2	应用软件系统用户培训	软件的使用方法及培训	不少于 1 天	操作及应用人员	线上

针对以上培训要求，制定了针对分局系统服务采购项目的具体培训计划，详情如下所示：

培训计划：

(1) 培训对象

针对拟使用本系统的分局民警。

(2) 培训地点

客户的管理人员和操作人员对系统使用的熟练程度是确保系统正常运行的重要前提条件，用直观、明确的讲解方式使接受培训的人员得到最有效的能力提升，达到最佳的培训效果。

培训地点：警务合成作战大队会议室线上远程培训。

(3) 培训目的

通过培训使得确保系统的正常运转，使参与培训的人员能了解本项目中的软件系统结构、性能等系统知识和产品功能知识，操作人员能对软件系统进行熟悉的操作、维护，并进行简单故障排除。

3、技术支持

供应商要提供全天候的技术支持

- (1) 就系统升级、维护、技术及安全方面给予建议、指导和支持；
- (2) 为项目提供良好的工作运行环境，包括建立、拷贝、备份测试环境，安装补丁等。
- (3) 负责软件的缺陷的追踪、缺陷补丁程序的确定、补丁程序的安装。
- (4) 系统正式运行后，该小组将转化为系统运行维护与技术支持。

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。

(7) 建立项目协调机制

供应商将在项目各阶段提供详细的进度安排、每周提供项目进度报告，并定期与我局召开项目协调会，商讨解决项目出现的新情况、新问题。

(8) 提供详细的项目支持档案

厂家将详细记录项目各个环节的书面档案，包括出现的问题、现象解决的时间、解决方法等详细的细节。该档案一式两份，一份由厂家保管，一份交我方保管。

六、项目投资

6.1 项目资金预算

投资用于全景云开查询系统 SaaS 服务，服务期 1 年，具体服务内容如下：

序号	基本服务项目	服务模块	服务内容	单位	数量	价格(元)
1	登陆账号	使用者账号	最大许可数指允许在同单位内共享的账号数量	个	1	118800
	全息档案	实人档案	人员信息：包括人员姓名、身份证、籍贯、性别、年龄等信息。	次	10000	
			基础信息：包括银行名称、银行卡号、预留手机号等信息。			
			线下消费：包括银行名称、银行卡号、预留手机号等信息。			
			云闪付转账：主要为云闪付转账信息。			
			银联全流水：包括多收单机构的交易信息、于 VX/ZFB 交易信息、ATM 机跨行转账及取款信息。			
		设备档案	多码查询、设备信息、画像分析、码值信息、轨迹信息、常连 WiFi、常连 IP、WiFi/IP 同网关系人、应用分析。	次	10000	
		IP 档案	对指定 IP 下的设备进行分析、筛选、查询、提数。	次	10000	
		WiFi 档案	对指定 WiFi 下的设备进行分析、筛选、查询、提数。	次	10000	
APP 档案	对指定 APP 下的设备进行筛选、查询、提数；并分析目标应用在境内境外的安装情况以及首装人群。	次	10000			
2	研判工具	地理围栏	通过在地图上选择指定区域对其进行布控，从而获得布控时间范围内出现在此区域内的设备信息。	次	500	
		WiFi 围栏	通过在地图上选择指定区域对其进行布控，从而获得布控时间范围内出现在此区域内的 WiFi 设备。	次	500	
		APK 解析	通过上传 APK 文件，分析其风险 URL、APP 信息、获取权限等内容。	次	500	
服务期限		自账号开通之日起，服务期为 1 年。				

价格(含税, 税率: 6%)	118,800 元	¥(人民币元 整)	壹拾壹万捌仟捌佰元整
-------------------	--------------	--------------	------------

项目服务期限 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。

6.2 资金来源与落实

本项目资金来源为区财政拨款, 项目资金全部用于购买全景云开系统服务, 服务期限为 1 年。