基于移动警务的人员身份核查核录系统

蔡玉鑫 巩思亮 杨 明 汤志伟 赵 博
(公安部第三研究所物联网技术研发中心 上海 200000)

摘 要 在信息化、动态化的社会条件下,如何维护社会治安、加强基层基础建设,已成为当前公安机关亟待解决的问题。文中结合公安实战需求,以进一步提升公安机关反恐维稳、重大活动安保和治安防范能力为目标,以情报平台为支撑,构建了基于物联网等先进技术和公安网安全接入的“云”-“管”-“端”一体化移动警务人员身份核录系统,实现了面向不同应用场景的多种形式的移动核录终端安全接入机制和信息安全保护策略,既降低了公安相关业务的执行成本,又提高了工作效率,创造了一定的经济效益和社会效益。

关键词 情报平台,核查核录,安全接入,“云”-“管”-“端”,反恐维稳
中图法分类号 TP391 **文献标识码** A

Personnel Identification System Based on Mobile Police

CAI Yu-xin GONG Si-liang YANG Ming TANG Zhi-wei ZHAO Bo
(The Third Research Institutute of Ministry of Public Security, Shanghai 200000, China)

Abstract Under the conditions of informationization and dynamic society, how to maintain public security and strengthen grassroots infrastructure has become an urgent issue for the public security organs. This paper combined the needs of the actual police to improve the public security organs' anti-terrorism stability, major activities security and public security prevention capabilities, and built a “cloud”-“pipe”-“end” mobile identity police verification system based on the advanced technologies of public security network and security access. The system implements various forms of mobile IP terminal security access mechanisms and information security protection strategies for different application scenarios, not only reduces the cost of public security-related business, but also improves work efficiency, createing certain and social benefits.

Keywords Intelligence platform, Verify and record, Secure access, “cloud”-“pipe”-“end”, Anti-terrorism stability

1 引言

当前,社会正处于快速转型期,群体性事件突出,刑事犯罪和社会治安问题多发,公安机关以打击查处为主的传统警务工作在有限的警力情况下面临巨大挑战。在信息化、动态化社会条件下,人员的流动更加频繁、迅速,虽然公安机关对重点人员的旅客订票信息、旅店住宿登记、网吧上网记录、卡口车辆通行记录、监所关押登记等动态轨迹信息的掌控作用明显,但重点人员的漏管漏控现象依旧严重。

目前,公安警务工作中,人员信息的核查一般分为两种方式:人工笔记核录和警务通核录。人工笔记核录方式的核录过程缺乏智能化和全方位化,日常执法工作效率低下且管控效果不佳;警务通核录是目前较常用的信息化核录方式,但该方式下部分警务通存在诸如只支持离线核录、核查数据更新繁琐、专机专用、一机单用等问题。

鉴于以上两种方式都未能建立有效的人员防控网、人员信息核录及管理技术较为落后等问题,本文依据各地公安机关关于加强基层基础建设的要求,依托情报平台,提出了建设一套涵盖接入安全管控平台和移动警务终端装备的“云”+“管”+“端”一体化应用方案的移动警务核查核录系统,该系统对进一步加强治安卡点、车站、码头、机场和人员流动大的重点部位人员基础信息采集和重点人员查控工作,增强对重点人员、重点车辆轨迹的管控能力,补齐现有实名人员管控的短板,进一步织密重点人员管控网络,全面提升公安机关情报预警能力有重要意义。

2 系统架构设计

系统整体应用架构如图 1 所示。

图 1 公安移动警务人员身份核查核录系统总体架构图

本文受 2018 年国家重点研发计划项目(2017YFC0806506)资助。
蔡玉鑫(1989—),女,硕士生,高级工程师,主要研究方向为移动警务、图像算法处理,E-mail:caiyuxin_good@163.com。

公安移动警务核查核录系统是结合公安实战需求，以进一步提升公安机关反恐维稳、重大活动安保和治安防范能力为目标，以情报平台为支撑，所建设的涵盖车站、码头、重大活动场所、固定治安卡点、党政机关、企事业单位以及街面的信息采集暨身份核录系统，该系统依托多样化的信息采集核查终端设备，实时采集和掌握重点区域、部位的重点人员和准重点人员的行动轨迹，开展重点人员查询比对等工作，逐步形成覆盖社会面的重点人员信息采集、核查网络，实现重点人员的全方位、立体式管控。

2.1　系统逻辑架构

移动警务人员身份核查核录系统从逻辑架构上采用可扩展的 B/S 三层结构，数据访问与业务逻辑分离，当数据库服务器更改以后，只需要更改数据访问的代码，而业务逻辑不变，因此不需要更改或重新编译业务逻辑层。系统总体分为 4 层：表现层（Presentation Layer，PL）、业务逻辑层（Business Logic Layer，BLL）、数据访问层（Data Access Layer）和数据库/其他业务系统。系统逻辑架构框图如图 2 所示。

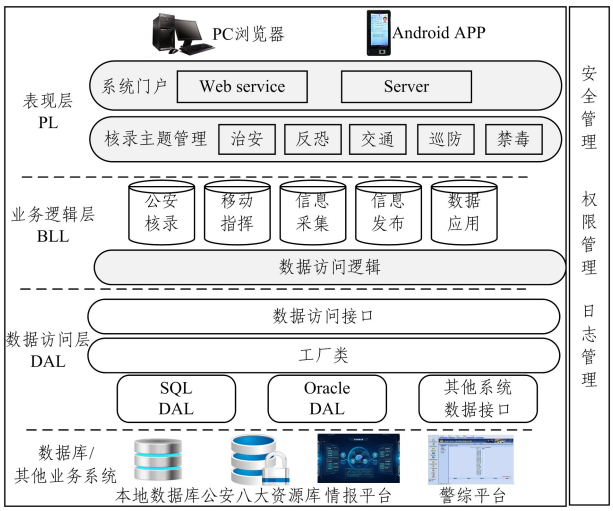

图 2　人员身份核录系统逻辑架构

2.2　系统服务模型

移动警务人员身份核查核录系统是一个以数据和信息服务为中心的、端到端整合的系统。为了实现对不断变化的公安业务的快速应对、防止一个业务模块的变化影响到另一个业务模块、实现系统组件之间的松耦合和信息共享，系统采用了面向服务的体系结构（SOA）。

系统服务模型如图 3 所示。

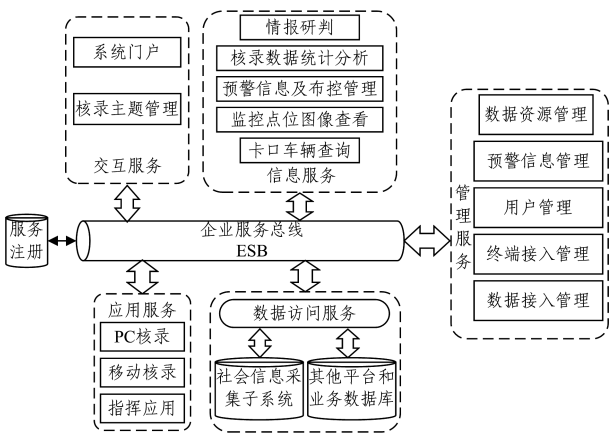

图 3　人员身份核录系统服务模型

SOA 组件模型将不同的业务服务组件通过良好的接口和规则关联起来，随着需求的变化，各松耦合的组件可以通过网络进行分布式部署、组合和使用。相比传统的信息化行业解决方案，面向服务的体系结构更加灵活，更容易适应业务快速变化的需求，同时，当某类服务组件的内容、形式和实现改变时，整体的架构和其他服务组件不会受到影响，实现了整个系统的灵活性、稳定性、可重用性和可扩展性。

2.3　系统数据流模型

移动警务人员身份核查核录系统从本质上讲是数据采集与汇聚、信息提取与处理、数据和信息展示与应用的系统。因此，ETL（Extract-Transform-Load）必不可少，ETL 是数据抽取、清洗、转换、装载的过程，是构建数据仓库的重要一环，用户从数据源中抽取所需要的数据，经过数据清洗，最终按照预先定义好的数据仓库模型，将数据加载到数据仓库中。数据与信息是移动警务人员身份核查核录系统运转和应用的核心，随着时间的推移，核录系统中的数据量会成倍增长，这些数据蕴含着巨大的价值和线索，因此，如何通过各种技术手段将数据转换为信息和有用的线索，成为衡量本项目可用性的主要标准。数据流模型如图 4 所示。

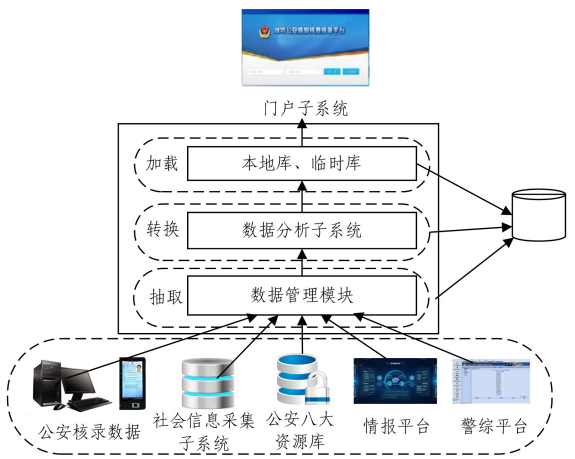

图 4　人员身份核录系统数据流模型

3　系统功能实现

本系统研究和实现了一套涵盖接入安全管控平台和移动警务终端装备的“云”+“管”+“端”一体化应用方案和融合服务模式，主要完成了移动警务核查核录云服务平台构建和移动警务核查核录终端软件开发。

3.1　移动警务核查核录云服务平台

移动警务核查核录云服务平台能够接收和处理移动警务核查核录终端采集上传信息，并提供查询比对服务的信息化平台，系统分为系统门户子系统、管理子系统和核录子系统。平台总体组成架构如图 5 所示。

（1）系统门户子系统主要由门户界面和核录主题管理模块组成。门户界面是用户接入系统平台的直观接口，本系统的门户界面具备核查核录软件安装、终端注册、通知通报、统计分析、门户功能模块展现等功能。

（2）管理子系统具备警示信息管理、数据资源库管理、用户及权限管理、终端设备接入、安全控制管理等功能。其中，数据资源库管理模块提供数据处理工具，通过数据抽取、标准化接口服务等方式，实现与公安部八大资源库、情报平台重点人员库以及警综嫌疑人员库的对接，来建立支撑移动核录系

统所需的标准化的统一比对资源库，并可以通过与情报、警综以及其他业务系统的对接，来对外提供人员、车辆等背景信息、轨迹信息的关联查询应用。用户及权限管理模块实现对组织机构信息及用户信息的新增、修改、删除、添加及初始化功能，系统支持市局、分县局、基层所队三级用户，市局、分县局两级管理员角色定义，市局管理员可通过权限中心实现对平台功能的授权管理，分县局管理员可在自己的权限范围内对下辖用户授权管理。终端设备接入管理模块能够支持各类移动、固定终端设备的接入及应用，并对接入设备在线状态、运行状况、安全注册、紧急注销等功能服务进行管理。安全控制管理模块能够针对公安网、VPN 专网、互联网、离线核录几种不同的核录终端提供安全的接入、设备管理、紧急注销、数据毁灭等安全控制服务，接入方式符合公安部的安全接入要求。

(3)核录子系统具备固定终端核录、移动终端核录等功能。固定终端核录通过配备二代证识别设备进行核录，移动核录模块提供无线核录相关的支持服务，用户可以通过已有移动终端调用后台服务接口来完成信息核录，移动核录功能提供对人员、车辆的核录。

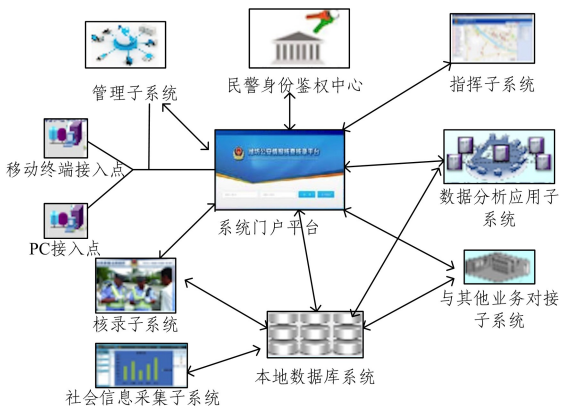

图 5 核录系统平台总体组成架构图

3.2 移动警务核查核录终端

移动警务核查核录终端执行核查核录业务的应用程序，进行二代身份证信息采集和查询。移动警务核查核录终端具有数据同步、PKI 认证、在线核录、离线查询与核录、集成身份证识别仪、集成指纹采集仪、拍照图传、GPS 定位与坐标采集等功能。

结合终端时钟和 GPS，核录信息数据自动进行时空关联。同时，附带身份证拍照识别、车牌拍照识别软件，在不借助其他手段的情况下，民警可以通过拍照智能快捷地获取身份证号和车牌号。

4 平台安全设计

由于移动警务人员身份核查核录系统具有离线和在线获取公安敏感数据的功能，因此需要建成一个全方位、多层次的安全服务系统。本系统实现了终端安全、通信安全、应用安全和网络隔离等安全功能。

4.1 终端安全

移动警务核查核录终端面临的安全风险主要有非法终端接入、非法人员接入、通信链路不安全、手机遗失后导致的违规接入等。针对这些安全风险，移动警务核查核录终端采取的安全措施包括移动警务终端安全操作系统、安全中间件、终端设备准入、无线 VPDN 技术、身份认证、加密传输、终端无信息存储等。

(1)移动终端设备准入。移动终端设备准入可通过两种方式来实现：运营商提供登录账号和密码，只有在其注册并审批通过的手机才能连入；手机终端信息在平台上注册，只有注册后才可接入。

(2)无线 VPDN 技术。在无线通信链路上采用 VPDN 技术，其租用公网通信链路，但与其他网络在逻辑上严格隔离。且移动终端在建立与平台链接过程中，只获得一次私有 IP，并在登录至链接建立的整个过程中都不能访问其他网络，尤其是互联网。

(3)身份认证。移动警务核查核录终端上使用的安全 TF 卡必须首先在平台身份认证系统中进行制证，并经过鉴别评估管理服务器注册之后才能使用。使用移动警务客户端拨通移动 VPN 接入网关调用安全 TF 卡时，会要求用户输入安全 TF 卡的 PIN 码，口令正确后，移动 VPN 接入网关和安全 TF 卡进行双向的证书认证，之后才能建立安全连接，从而保证用户身份的合法性，否则根本无法接入平台，无法使用移动警务功能。

(4)加密传输。空中无线传输的信息，由 VPN 客户端和移动 VPN 接入网关之间建立的加密隧道进行保障，采用 SSL/TLS 协议实现，并采用 SM1 加密算法。

4.2 通信安全

通信安全通过采用安全的密钥管理方案、SM1 加密算法和数据加密封装传输实现了通信过程的机密性和完整性。该密钥管理方案通过了国家密码管理局专家的安全性审查，认定为安全的密码管理方案，而且数据加密封装和传输协议也经过国家密码管理局专家的审查，认定为安全传输协议。

公安用户使用移动终端通过上网(TCP/IP)方式获取公安信息网资源需经过移动 VPN 接入网关，移动 VPN 接入网关验证访问者的身份，阻止非法用户的进入(防止入侵和攻击)，并为合法移动用户建立安全通信隧道，保证移动终端与后台网络之间的数据在公网路段上传输的安全。

4.3 应用安全

应用安全通过两个方面来实现：1)接入终端对应用服务系统的查询，应用服务系统提供的应用安全措施；2)应用服务系统需要对公安网信息进行获取，通过网闸提供应用层的安全措施。

4.4 平台安全

接入平台在移动公网边界部署防火墙，可以防范网络攻击。移动 VPN 接入网关提供了接入设备的安全认证功能，因此可以抵制非法用户的访问。两种方式相结合可以确保平台在移动公网边界的安全。

在内网，集中监控与审计系统对安全接入系统内的业务、应用、设备、数据等各个层面进行管理和监测，能够及时发现各类违规和异常情况，并提供强有力的追踪审计功能，对内网应用接入安全进行集中管理。其工作原理如下：管理员首先对业务进行注册，按照单位、业务、设备、链路、协议等层次进行注册。注册的业务通过编译后转换成为规则，该规则用来区分业务种类和判断流量合法性。所有未注册的业务均为非

法业务。通过部署监管探针对接入系统流量进行收集，匹配规则并进行分类。将未匹配的流量上报为异常流量，并告警。同时，接入区也集中收集和分析主要安全设备的业务日志，如移动 VPN 接入网关、移动应用代理服务器等。

5　实验

本文对系统进行了功能测试和性能测试。

在功能测试中，针对系统平台进行了 APK 安装、通知通报、统计分析、信息比对查询、操作日志、用户及权限管理、设备管理等测试，针对移动警务核录终端进行了数据同步、PKI 认证、在线/离线数据查询与核录、身份证识别、拍照图传、GPS 定位与坐标采集等测试。

在性能测试中进行了在线用户数和用户并发数、简单事务响应、复杂事务响应等测试。测试结果为：平台支持的在线用户数大于等于 500 个，且用户并发数大于等于 50 个；简单事务响应（包含数据上载接收、轨迹查询等）的响应时间小于等于 5 s；复杂事务响应（如分级统计等）的响应时间小于等于 60 s，在分级统计测试中分别记录统计了 1 000 条、10 000 条、100 000 条、1 000 000 条核录数据，结果如图 6 所示。

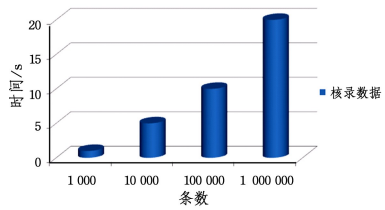

图 6　平台统计核录数据所需时间测试图

结束语　移动警务人员身份核查核录系统充分发挥了科技信息化在公安工作中的支撑及引领作用，以信息技术推动警务工作转型升级、科学发展，显著提升了公安信息化建设水平。在社会效益方面，本系统除可以起到犯罪的事前预防和事后线索挖掘之外，还可以降低公安相关业务的执行成本，提高工作效率和拓宽工作能力，有利于提升公安机关维护社会稳定的能力和增加人民群众对于公安机关的信任度与支持度，除了可以创造直接经济效益之外，所能创造的社会效益和挽回的损失是无法用金钱估量的。

参 考 文 献

[1] 李洪，渠凯. SSL VPN 安全方案与发展趋势分析[J]. 电信技术，2011(1).
[2] 吴世忠. 信息安全保障[M]. 北京：机械工业出版社，2014.
[3] 彭发喜. 大中型企业信息安全体系架构研究[J]. 信息与电脑(理论版)，2017(17).
[4] 蒋敏慧，钟磊，李楠，等. 无线网络用户行为安全管理设计[J]. 信息系统工程，2017(7).
[5] 段瑞霞. 基于智能终端的移动审批应用研究[J]. 数字技术与应用，2016(11).
[6] 刘建. B/S 系统中应用公钥证书的技术研究[D]. 济南：山东大学，2006.
[7] 邱鹏飞. B/S 架构下一次性口令身份认证方案的设计与实现[D]. 太原：太原理工大学，2008.
[8] 蒋华，姚莹，鞠磊. 服务链中可认证的组密钥管理方案[J]. 计算机应用研究，2018，(6)：1-2.
[9] 宋钰. 基于 SOA 架构的企业信息系统集成的研究与应用[J]. 电子技术与软件工程，2019(3)：256.
[10] 周瀚章，冯广，龚旭辉，等. 基于大数据的 ETL 中的数据清洗方案研究[J]. 工业控制计算机，2018，31(12)：108-110.
[11] 翁业林，周泓，侯兵. 面向企业级数据中心的分布式 ETL 研究与设计[J]. 软件工程，2018，21(12)：15-18.
[12] 饶宏博，石磊. 基于 B/S 架构安全检查管理平台建设方案[J]. 智能计算机与应用，2019，9(1)：257-258，261.
[13] 洪小龙，陈崇平. 视频网终端安全准入系统的设计与实现[J]. 广东公安科技，2018，26(4)：5-7.
[14] 孙艳丽. 无线宽带 VPDN 技术及其应用的研究[J]. 数字通信世界，2017(3)：198-199.
[15] 赵荣辉，王瑜琦. 新一代移动警务即时通信消息互联方案[J]. 警察技术，2018(6)：53-56.
[16] 刘宏舸. 移动警务终端技术的要求及发展趋势[J]. 数字技术与应用，2018，36(10)：224-225.
[17] 韩秀德，陈昌前. 移动警务信息资源跨网络边界安全共享策略研究[J]. 警察技术，2018(5)：43-46.
[18] 王亮，周仁贵，廖承斌. 多模智能移动警务终端在公安情勤指一体化中的应用[J]. 警察技术，2018(6)：57-60.