智慧城市建设与大数据安全问题研究

徐明慧　金乐　冯霄鹏

(北京电信规划设计院有限公司,北京 100048)

摘要: 通过对智慧城市建设总体架构、大数据安全等内容进行研究,归纳整理了智慧城市建设过程中面临的大数据安全问题。通过分析大数据安全问题产生的原因,给出提升大数据安全能力的方案建议,从而保证智慧城市建设中真正实现数据融通、信息安全,进而促进智慧城市建设持续、健康发展。

关键词: 智慧城市; 大数据; 大数据安全; 人工智能

1　引言

随着“网络强国”战略、“大数据”战略、“互联网+”行动计划的实施和“数字中国”建设的不断发展,我国智慧城市建设步伐不断加快。截至 2019 年年底,我国开展智慧城市建设试点的城市近 800 个[1],成为全球智慧城市知名国家。

智慧城市建设[2]可实现数据融通、协同、渗透,更好地服务城市和人民。然而,随着智慧城市建设中大量数据在系统中集中存储,大数据安全风险不断集中、突出,如身份认证、电子证照等基础通用能力模块被各类应用广泛使用。一旦这些应用被成功攻击,将导致巨大的损失,甚至威胁到城市安全、社会安全和政府安全。

2　智慧城市建设与大数据安全

2.1　智慧城市建设

智慧城市建设[2]主要是通过大数据、云计算、物联网、人工智能等新一代信息技术,推动政务、产业和民生几大领域的信息化建设,进而实现全程全时的为民服务、高效有序的城市治理、共融共享的数据开放、绿色开源的经济发展,以及安全清朗的网络空间,最终实现国家与城市协调发展的新生态。

智慧城市建设的总体架构主要由感知层、网络层、数据层、平台层、应用层等构成。其中,数据在智慧城市建设中的流通路线为: 感知层获取数据,网络层进行数据传输交互,服务层为海量数据存储、实时分析和处理提供服务,平台层实现数据之间的聚合、融通,应用层面向最终用户提供基于数据融通的智慧化服务。具体的智慧城市解决方案架构图以及建设中的数据流转图分别见图 1 和图 2。

2.2　大数据安全

随着大数据、云计算、物联网、人工智能等技术的快速发展,全球数据量出现爆炸式增长; IDC 研究的“大数据摩尔定律”表明,人类社会产生的数据一直在以每年 50%的速度增长,也就是说,每两年就增加一倍。在大数据不断向各个行业渗透,深刻影响国家的政治、经济、民生和国防的同时,其安全问题也将对个人隐私、社会稳定和国家安全带来巨大的潜在威胁与挑战。

大数据安全[3]是要确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。传统而言,企业或单体场景下的大数据安全自下而上可依次分为大数据平台安全、数据安全和个人隐私保护等 3 个层次。大数据平台不仅要保障自身基础组件的安全,还要为运行其上的数据和应用提供安全机制保障; 除平台安全保障外,数据安全防护技术为业务应用中的数据流动过程提供安全防护手段; 隐私安全保护是在数据安全基础之上对个人敏感信息的安全防护。

3　大数据安全问题产生的原因

3.1　智慧城市建设中的大数据安全问题

智慧城市建设中涉及到的数据具备种类多、覆盖

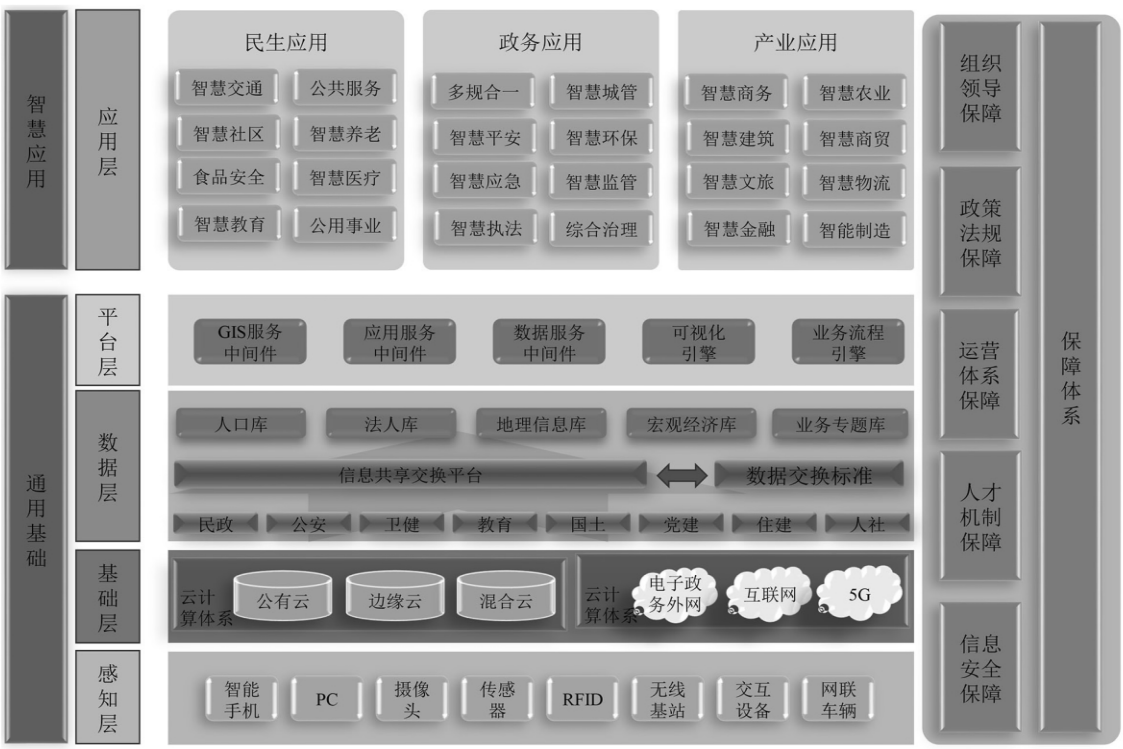

图 1　智慧城市解决方案总体架构

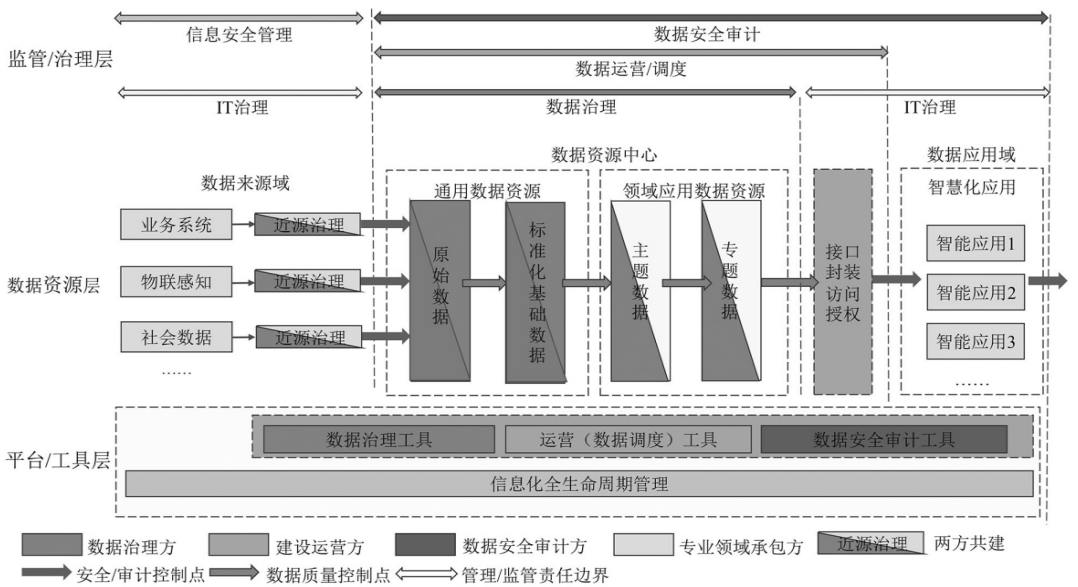

图 2　智慧城市建设中的数据流转

范围广、数据量大、价值密度低、总价值量巨大等特点。既包扩底层传感器数据、视频采集数据等在内的物联感知数据，也包括公民、企业等单位产生的移动通信数据，还包括各类城市运营管理部门产生的政务、公共服务运行、市场主体行为等数据。智慧城市建设正在朝感知泛在化、连接全面化、能力通用化和应用智能化方向快速发展，正在越来越深入地影响城市中各类主体的生产和生活，也为大数据安全提出了大量新的挑战。

(1) 感知泛在化，即大量具备联网功能的传感器承担了智慧城市运行当中的大量信息感知功能，对人

工填报、人工采集的信息构成了替代。大量物联感知和控制设备的广泛部署意味着大数据安全的分析视角必须从平台层向网络和前端感知层延伸，物联感知设备遭到大规模劫持和控制已呈频繁发生且不断加剧的态势。这种控制不仅可以用来制造垃圾流量、发起 DDOS 攻击，也可以通过人为伪造传感器数据从而成体系地干扰整个智慧化的运行机制，例如黑客如果大规模劫持了某区域的消防传感器控制或者接入平台，则可以在发生重大事故时故意发送大量虚假警报，从而严重干扰救灾救援业务。

(2) 连接全面化，即各类垂直应用系统之间、各类设备与设备之间通过各类网络产生了大量连接。这意味着跨系统、平台、网络环境的大数据应用是新型智慧城市运行中的常态，并在平台层为大数据安全提出了大量新的挑战。一是，所有的跨系统、平台、网络环境边界天然成为潜在的安全风险来源。例如，在跨网络数据交换的场景下，攻击者可以通过网络嗅探的方式获取交换边界的身份认证密钥，从而伪装成正常的数据交换方，从低密网络发起对高密网络的数据交换请求，从而导致数据泄露; 二是，各类数据交换、流转往往脱离原始数据提供方的控制，攻击者存在通过不同来源数据进行碰撞获取被保护信息的可能。例如，在医疗场景下，数据交换需要对于患者的身份信息进行脱敏加密，但有时交换数据中会包括移动平台的账户加密字符串，这个字符串可以利用数据黑市上的数据集进行碰撞，从而获知患者的具体身份信息，从而获取患者的就诊、治疗等高度敏感的隐私数据。

(3) 能力通用化，即诸多共性能力被通用平台逐步取代，各种信息系统烟囱被逐步打破。某种程度上说，这种通用化趋势对于大数据安全具有双刃剑的作用，一方面高度集中的云平台、中间件和大数据平台可以提供较强的数据安全防护能力; 另一方面，数据湖、数仓、数据中台等数据资源层建设也将各种来源的数据集中起来，为数据分级、分类、精确的权限生命周期管理和安全审计提出了更高的要求。从目前的实践来看，大量数据资源中心难以做到权限的范围和生命周期与访问行为的范围和生命周期精确匹配，研发分析人员多人共用账户、超出业务需求访问数据，甚至下载泄露的事件时有发生。

(4) 应用智能化，即人工智能算法正在进入大量应用场景，并且逐步从决策支持向(部分) 自主化运行渗透，各类智能算法在城市感知认知过程当中逐步占据更为重要的基础性地位，其算法的安全性就成为了新的大数据安全分析视角下必须关注的问题。其中，既包括算法本身的安全问题，如基于对抗生成网络技术的算法攻击手段可以利用在车牌上添加人类肉眼不易辨别的花纹从而欺骗视频监控场景下的车牌识别 OCR 算法; 也包括针对基于算法的公共服务进行攻击，如隐私差分算法可通过部分公共服务接口提取个人隐私; 还包括基于人工智能算法的跨领域综合性威胁，例如内容推荐算法定向推送敏感内容从而危害社会安全稳定。

3.2 大数据安全问题的原因分析

由上可知，随着智慧城市的建设越加深化，其对应的大数据安全挑战也愈加严峻，主要原因归结为以下几方面。

(1) 安全理念严重滞后。实践中，以合规为导向的安全理念仍然占据主流，缺少从底线思维出发的整体安全理念; 大家对于新攻击形态、新威胁类型认知不足; 数据安全部门和业务部门之间的关系以监管和被监管为主，协同意愿和机制较为欠缺。

(2) 智慧城市建设相关的标准和数据安全机制不健全[4]。目前，缺少针对智慧城市建设运行中产生的大量异构数据的精细化的分级、分类管理标准，缺少对于数据流转溯源、行为审计追踪的技术和管理标准，缺少对于大数据安全和算法相关的安全问题的安全风险评估标准和方法论。

(3) 大数据安全运营人才持续匮乏。相对基于技术层面对抗渗透的人才，能够持续监督优化智慧城市整体安全运营，特别是数据资源安全运营的人才非常稀缺。大数据来源多样化、数据范围广泛，数据在流转、应用过程中产生聚合产生新的数据资源体系，往往会与原始数据保护边界发生变化，如何在整个数据资源的流转体系中进行大数据资源的合理安全防护，对于安全运营人员提出了非常高的挑战和要求。一方面，要求安全运营人员对于数据的业务属性具有深刻理解，能够识别其中蕴含的安全风险和信息价值; 另一方面要求安全人员根据数据的需求场景，选取风险暴露和技术投入、管理难度多要素平衡的技术方案，在安全可控的前提下尽可能发掘、实现数据价值。

(4) 系统复杂度高速膨胀，对于管理体系造成冲击。智慧城市是一个典型的大规模异构系统，其建设

在时空和管理两个维度均存在高度离散化的特征。各个建设主体往往在设备选型、通信协议、数据治理、接口规范、业务标准、安全措施等方面存在大量差异,难以进行整体化治理,导致大量数据、服务、设备、系统采取私下对接或临时性接入的模式流转,难以纳入统一安全体系,造成管理盲区和治理黑洞。

4 提升智慧城市大数据安全能力

智慧城市建设步伐加快,各地纷纷重视智慧城市建设是好现象,但是一味地追求速度、规模,而不重视数据安全,将为后期的智慧城市运营带来一定的安全隐患,因此有必要从各个层级、各个方面重视数据安全。通过研究,本文建议重点从管理和技术两大方面来提升智慧城市大数据安全能力。

4.1 强化智慧城市大数据安全管理能力

(1) 建立基于整体视角的韧性安全理念。对于以智慧城市为代表的超复杂系统,难以完全消除发生数据安全事件的概率。所以,从理念角度上说,除了要从合规角度出发做好防护以外,还要树立风险必然发生的底线思维和韧性意识。在安全风险的评估、管理和运营中,既要注重预留安全余量,又要注重从业务运行循环的整体视角评估数据资源和智能应用的完整性、可用性、保密性。

(2) 完善智慧城市大数据安全标准。建立大数据资源的安全运营标准,针对数据资源固有的敏感性、保密性以及数据资源在不同场景下使用的安全风险建立量化的风险-收益评估标准,实现公共利益和数据相关权利人安全风险的平衡。在数据采集阶段,建立数据收集权限、范围的集中授权监管机制,明确哪些部门、哪些人员可以收集哪些数据;在数据汇聚阶段设立数据资源分级分类管理标准,对于存在安全风险的敏感数据采取加密、脱敏存储的形式,尽量避免原始数据在流转过程中多次落地存储;在数据挖掘和应用阶段,建立业务需求和场景化安全风险评估标准,明确何人在何种情况下可以调用哪些数据,建立数据权限生命周期管理标准,做到单次授权、单个对象,范围和属性的精细化权限管理,建立集中化的数据资源调用标准,对于数据的流转和调用进行全程留痕和审计。

(3) 完善智慧城市大数据安全制度保障。在组织机制上,建立网信办、大数据局、公安等多个部门参与的大数据安全管理联席机制。其中,数据资源管理部门承担双重角色:一方面,作为专门负责统筹新型智慧城市建设的综合性部门,对智慧城市大数据安全的议题承担最终需求方的角色,即承担各个零散需求部门和社会各方的大数据安全需求收集、评估、整理的需求侧运营工作,并根据公共利益确定大数据安全的整体需求;另一方面,承担数据融合共享为切入口的智慧城市大数据资源建设工作,作为技术标准制定、技术选型、运营机制等方面第一手的管理方和监管方,是事实上的供给侧运营部门。此外,为了更好地保障大数据安全运营工作的成效,应积极探索“管运分离”的长效化运营机制。

(4) 注重产业化合作,激活多主体合作活力。在智慧城市建设运营框架下,探索安全运营的政企合作机制,吸引社会力量投入共建共管共享,引导市场主体形成新型智慧城市整体安全运营商;强化公民权利意识和公共数据安全意识、提升社会认同感和支持力度、完善数据安全确权体系和知情同意溯源体系、推广社会公众体验感知等。

(5) 强化相关保障支撑,加强人才队伍配套建设。建立基于综合大数据安全的专业化人才培养体系,进一步推动安全认证培训从合规导向向整体安全运营导向演进;建立从全方位安全对抗视角出发的大数据安全人才培养机制,充分利用军民融合、政企合作等方式建立综合性人才梯队。

4.2 关注新兴技术,升级大数据安全保障工具箱

(1) 在网络层,加快推进 IPv6 等新型协议的部署应用,逐步淘汰安全性不足的老旧协议和组网模式,构建不可抵赖的网络追踪溯源机制。

(2) 在设备层,强调边缘设备的本质安全,采取区块链等手段构建设备标识体系,构建设备对设备、设备对系统的可信连接模式,推动计算、网络、存储等底层 IaaS 设备完成全面的自主可控替代。

(3) 在数据的传输和存储层[5],注重隐私和敏感数据的全面脱敏加密;合理构建云、边协同的数据存储和应用模式;引入联邦学习等新兴技术模式,减少敏感数据在网络中的低效搬运;全面推广数据不落地,可用不可见的服务化封装模式;利用区块链智能合约等新兴技术手段,推动公共数据资源上链,构建数据资源溯源标记,实现数据的全流程可审计。

(4) 在平台层,进一步推动国产化操作系统在专业应用领域的覆盖。通过智能合约等手段强化系统间

的协同;构建支持多种数据共享交换模式的接口封装审计技术,将全量大数据的共享交换流转纳入审计范围,做到全流程安全可控;强调零信任和本质安全理念,充分推进虚拟化技术,将存在较大数据安全风险的研发活动置于可信的沙箱环境下进行;构筑基于大数据分析的安全态势感知体系,建立对于大数据安全风险的主动感知和管控机制。

(5) 在应用层,注重关注智能算法的算法安全机制。重要的基础识别算法采取加密分发、定期迭代的部署模式,在关键数据采集领域逐步替代采用固定版本识别算法的硬件设备;对于交通调度、物流调度、能源调度等涉及城市重要公共运行业务的核心算法进行全流程加密和定期更新,避免因核心算法泄露导致的综合性攻击风险。

5 结束语

基于大数据的智慧城市建设,关系着每个人的生活,为人们的生活提供方便,但其中的大数据安全问题需要引起全员重视。智慧城市建设,首先需要所有参与建设、实施、运行等各阶段的人员对大数据安全问题达成统一共识,共同关注大数据安全问题;其次需要完备的加强大数据安全的规章制度,并在智慧城市建设中的每个层级规避大数据安全问题;最后需要持续加大培养大数据安全人员的力度,提高大数据安全技术的普及度。从而从全方位、多角度、多层级来保障智慧城市建设持续、健康发展。

参考文献

[1] 前瞻产业研究院. 2020 年中国及 31 省市智慧城市试点及建设情况汇总[EB/OL]. (2020-06-18) [2020-09-24]. https://www.qianzhan.com/analyst/detail/220/200617-f9f0154d.html.

[2] 王兆庆, 贺勇. 以大数据为支撑的智慧城市建设研究[J]. 物联网技术, 2018(1): 46-48+50.

[3] 周蓉, 陈印, 唐权. 基于大数据的智慧城市建设信息安全研究[J]. 信息通信, 2016(8): 132-133.

[4] 佟大柱. 智慧城市中的大数据安全问题研究[J]. 信息与电脑(理论版), 2019(3): 214-215.

[5] 周振邦. 大数据与云计算的安全问题及解决思路分析[J]. 科技传播, 2019(6): 155-156.

作者简介:

徐明慧 北京电信规划设计院有限公司高级经济师、注册咨询工程师(投资),主要从事通信、智慧城市等领域的研究与咨询工作

金乐 北京电信规划设计院有限公司工程师,主要从事通信、智慧城市等领域的研究与咨询工作

冯霄鹏 北京电信规划设计院有限公司高级工程师,主要从事数据通信网络、互联网、数据中心、区块链、智慧城市等领域的规划和咨询设计工作

Research on smart city construction and big data security

XU Minghui, JIN Le, FENG Xiaopeng

(Beijing Telecom Planning and Design Institute Co., Ltd., Beijing 100048, China)

Abstract: This paper summarizes the big data security issues in the process of smart city construction by studying the overall architecture. By analyzing the causes of big data security issues, it gives suggestions on how to improve big data security capabilities, so as to ensure the real realization of data integration and information security in the construction of smart cities, thereby promoting the sustainable and healthy development.

Key words: smart city; big data; big-data security; artificial intelligence

(收稿日期: 2020-09-24)