智慧城市项目中数据共享与数据安全问题研究

李　凡
武汉东湖学院　计算机科学学院　湖北武汉　430212

摘　要：科技技术的发展，推动了新型智慧城市建设步伐。数据作为实现智慧城市的基础支撑和核心驱动力之一，优化城市管理和服务，提升城市的竞争力与可持续发展。然而，智慧城市项目建设中面临着数据共享与数据安全问题。本文旨在研究智慧城市项目中的数据共享和数据安全问题，并提出相应的解决方案。

关键词：智慧城市；大数据；数据共享；数据安全；方案

Research on data sharing and data security issues in smart city projects

Li Fan
School of Computer Science, Wuhan Donghu University, Wuhan, Hubei 430212

Abstract: The development of science and technology has promoted the pace of the construction of a new smart city. As one of the basic support and core driving forces to realize the smart city, the data should optimize the urban management and service, and enhance the competitiveness and sustainable development of the city. However, the construction of smart city projects is faced with data sharing and data security problems. This paper aims to study the data sharing and data security issues in smart city projects, and propose corresponding solutions.

Keywords: smart city, big data, data sharing, data security, solution

一、引言

科技技术的发展，推动了以物联网、大数据、云计算、人工智能等新型技术为基础的智慧城市建设步伐。数据则成为实现智慧城市的基础支撑和核心驱动力之一。当前，智慧城市治理面临着数据共享与数据风险之间存在内在张力的问题[1]。数据共享可以帮助城市部门之间更好地协作和解决城市管理问题，但数据安全问题也需要考虑和处理。针对智慧城市项目中的数据共享和数据安全问题，本文通过文献综述法，结合笔者多年的智慧城市项目建设经验，提出了相应的解决方案。

二、智慧城市项目中问题

最近几年，许多学者对智慧城市项目中数据共享与数据安全问题进行了大量的研究，结合笔者多年的智慧城市项目建设经验，智慧城市项目建设主要面临以下问题：

（1）缺乏合作与治理机制：不同部门和机构在数据交换与共享中可能存在利益分配和权力平衡的问题，需要建立公正的机制来协调各方的利益，以便实现数据共享的顺畅进行。

（2）数据孤岛：存在着不同部门、机构和系统之间的数据孤岛问题，导致数据无法在不同系统之间流动和共享，这限制了数据的综合利用和价值发挥。

（3）数据非标准化：涉及多个领域和行业，各自拥有不同的数据结构和格式，需要制定统一的数据标准和接口规范，以实现数据的交换和共享。

（4）数据质量和一致性问题：不同系统之间的数据质量和一致性问题也是影响智慧城市数据交换与共享的因素。

（5）数据安全和隐私保护问题：涉及大量的敏感信息和隐私数据的交换，确保数据的安全性和隐私保护成为一个紧迫问题，需要建立数据安全管理机制和隐私保护政策等。

（6）数据访问权限与控制不明确：存在数据访问权限与控制机制不够明确或执行不力，会出现未经授权的

作者简介：李凡，男，湖北人，硕士，助教，单位：武汉东湖学院，研究方向：网络安全。

数据访问，甚至滥用和侵权的情况，需要明确的权限和管控机制，以避免未经授权的数据访问和滥用。

（7）缺乏风险评估和安全审计：系统的稳定性也至关重要，为了预先识别潜在的风险和漏洞，通过风险评估和安全审计，可以发现并解决软件中的缺陷和漏洞，防止数据泄露或滥用对社会造成损害。

三、数据共享和数据安全重要性

数据共享：智慧城市项目建设中涉及的数据涵盖了多种类型和来源的数据，例如个人身份数据、医疗健康数据、地理信息数据、交通数据等。这些数据需要跨部门、跨领域进行共享，才能充分挖掘和利用其价值，更好地服务于城市管理和市民需求。数据共享需要解决多种技术和政策问题。

数据安全：由于涉及大量个人隐私、企业商业秘密等敏感信息，智慧城市项目建设中的数据安全问题尤为重要。数据安全不仅需要技术手段的支持，还需要制定和实施相关法律法规和规章制度，加强数据保护措施，避免数据被泄露、滥用、篡改等。

四、数据共享和数据安全问题的解决方案

智慧城市中的大数据似一把双刃剑，数据的共享与流动有利于城市的管理与发展，同时数据的共享与流动也暗藏了数据安全的隐患[2]。针对智慧城市项目中的数据共享和数据安全问题，智慧城市项目可以从以下六个方面来解决：

1、法律方面：建立并执行相关的法律法规，明确数据的所有权、使用权限和责任。制定数据隐私保护法，规范数据的采集、存储、共享和使用，明确数据共享的要求和限制，加强对违法行为的处罚力度。

2、制度方面：建立健全的数据管理制度，明确数据共享的流程和标准。制定数据共享的审批和审核机制，加强对数据共享过程的监督和管理，确保数据共享的合法性和安全性。

3、组织方面：建立专门的数据管理部门，负责数据共享的监管和管理工作。制定数据安全管理制度，明确责任和权限，并加强内部沟通和协作，提高数据共享的整体安全性和效率。

4、企业方面：企业在参与数据共享时要加强自身的安全防护能力，建立完善的信息安全管理体系。加强数据共享合作伙伴的筛选和管理，签订明确的数据共享协议，明确数据的使用和保护要求。

5、人员方面：提高员工的安全意识和技能，加强培训和教育，加强对员工的监督和管理，建立相应的响应机制，及时发现和处置数据安全事件。

6、技术方面：智慧城市建设中，数据中心和大数据技术是至关重要的组成部分。传统集中式数据中心主要通过以下技术方案实现数据的交换和共享。

（1）ETL（Extract Transform Load）：支持数据清洗、转换和映射操作，使得不同系统中的数据可以相互交换和共享。常用的有Kettle、Datax、DataPipeline等。

（2）数据库同步工具：提供了不同数据库系统之间数据同步、复制和转换的功能，以确保不同数据库之间的数据一致性和共享。如数据同步工具之FlinkCDC、Canal、MySQL Replication等。

（3）API（应用程序接口）：通过定义标准化的接口和协议，如RESTful API或SOAP协议格式，并结合定时任务中间件Quartz、XXL-JOB、Elastic-job等实现不同的部门或企业系统之间的数据交换和共享。

（4）开放数据平台（数据中台）：提供一种集中式的数据存储和交换通道，以便不同的应用程序和用户能够访问和共享数据，可以为智慧城市的各个利益相关方提供便捷的数据访问和共享机制。

（5）消息队列中间件：相较于API（应用程序接口），最大优点是可以保证数据能及时在各个系统之间进行传递。常用的有RabbitMQ、Kafka、RocketMQ、ActiveMQ等。

集中式数据中心容易出现数据安全问题，需要通过数据加密技术、身份认证技术、入侵检测与防御技术等，并建立完善的数据备份和恢复体系等措施保证数据安全。

五、数据共享和数据安全问题的创新型解决方案

创新型的组织和新技术也是未来智慧城市项目建设发展趋势，目前在一些智慧城市项目建设中得到了一定应用，具体措施如下：

1、组织方面的创新

部分学者对深圳市S区智慧城市的个案进行研究，深入探讨了智慧城市建设中如何处理数据共享和风险防控之间的矛盾。深圳市S区智慧城市项目建设中，最关键的一环是在政府和市场之间搭建了国有企业A公司，建构了一个政府–国有企业A公司–市场的智慧城市数据协同治理模式。如图1所示，国有企业A公司上承深圳市S区，下接参与智慧城市项目建设的市场主体。在运作机制上，智慧城市的所有数据由国有企业A公司负责统一采集、传输、存储、利用，通过标准化建设和考核机制进行奖励和惩罚措施，提升了数据共享程度。与此同时，所有参与智慧城市建设的市场主体都必须通过国

有企业A公司的技术评估后才能开展工作。兼具公共属性和市场属性“双重身份”的国有企业A公司，成为政府和市场之间的缓冲地带，有效破解了处理数据共享和风险防控之间的矛盾[3]。

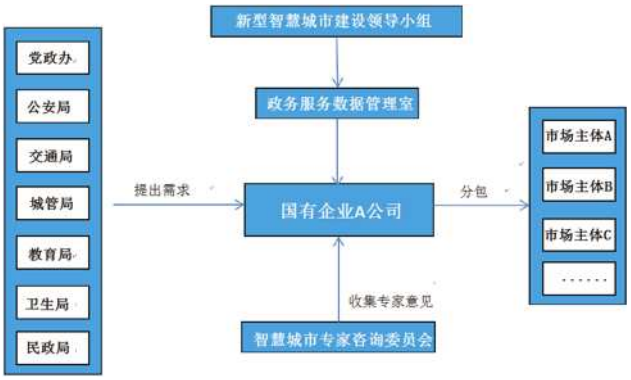

图1　深圳市S区新型智慧城市建设组织架构

笔者参与的广东省F市的智慧安全城市项目建设中，也采取了类似的组织架构管理模式，建立了一个广东省F市政府–国有企业公司–市场的智慧城市数据协同治理模式，很好的解决了智慧安全城市项目建设中数据共享和风险防控之间的矛盾。

2、技术方面的创新

在智慧城市建设中，传统的数据中心往往采用集中式的架构，此模式存在数据安全风险和隐私问题，为了解决这些问题，新型的分布式数据管理模式逐渐崭露头角，而区块链技术和隐私计算就是其中代表。

（1）区块链技术

区块链技术作为一种去中心化、安全可信的分布式技术，具有去中心化、透明性、不可篡改性、高安全性、匿名性等特点。这些特点使得区块链技术可以被应用于智慧城市的数据共享和安全保障领域。

公共交通：通过区块链技术，乘客可以安全地存储和管理个人出行数据，同时与城市交通管理部门分享必要的数据，这样的数据共享机制可以帮助城市更好地规划交通网络，同时保护用户的隐私。

卫生健康领域：智慧城市中的医疗机构可以利用区块链技术来安全地共享卫生健康数据。患者的医疗记录可以被加密存储在区块链上，并授权给特定的医疗机构进行访问。这样，不同的医疗机构可以更好地协作，同时保护患者隐私。

城市治理：智慧城市可以利用区块链技术来实施智能合约，通过区块链上智能合约的执行，可以简化许多繁琐的行政流程，如土地登记、权益分配等，并确保数据的安全性和不可篡改性。

通过区块链技术，智慧城市可以促进数据共享，提高数据安全性，并为城市居民提供更智能、高效的公共服务。

（2）隐私计算

2016年发布的《隐私计算研究范畴及发展趋势》正式提出“隐私计算”一词，并将隐私计算定义为：“面向隐私信息全生命周期保护的计算理论和方法，是隐私信息的所有权、管理权和使用权分离时隐私度量、隐私泄漏代价、隐私保护与隐私分析复杂性的可计算模型与公理化系统。”[4]

目前主流的隐私计算技术主要分为三大方向：以多方安全计算为代表的基于密码学的隐私计算技术；以联邦学习为代表的人工智能与隐私保护技术融合衍生的技术；以可信执行环境为代表的基于可信硬件的隐私计算技术。

多方安全计算MPC（Secure Multi-party Computation）：由图灵奖获得者姚期智院士于1982年通过提出和解答百万富翁问题而创立[5]，是指在无可信第三方的情况下，多个参与方共同计算一个目标函数，并且保证每一方仅获取自己的计算结果。

联邦学习FL（Federated Learning）：能够实现在本地原始数据不出库的情况下，通过对中间加密数据的流通与处理来完成多方联合的机器学习训练。

可信执行环境TEE（Trusted Execution Environment）：通过软硬件方法在中央处理器中构建一个安全的区域，保证其内部加载的程序和数据在机密性和完整性上得到保护。

隐私计算的三大技术路线各有优缺点（如表1所示），在政务隐私数据共享中应该结合应用环境选择合适的技术。

表1　隐私计算的三大技术路线优缺点

技术类别	数据保护	计算性能	计算模式	硬件依赖
多方安全计算	强	弱	分布式	否
联邦学习	中	中	分布式	否
可信执行环境	中	强	中心化	是

政务数据平台内数据共享：因政务数据平台内网络安全级别较高，数据以局域网传输为主，在数据传输安全有保障的前提下，可采用TEE技术，充分保障计算效率。

政务数据平台间数据共享：对此可采用FL+TEE技术，平台间数据交互采用FL技术，避免数据在传输过程中泄露。

政务数据平台与商业数据平台间数据共享。场景一：如商业数据为非隐私数据，则可通过API将数据接入政务数据平台，采用TEE技术进行计算；场景二：如商业数据为隐私数据，则根据商业平台能提供的技术类别，采用FL+TEE技术或MPC+TEE技术。

传统的集中式数据中心存在数据安全风险问题，而新型分布式数据管理模式（区块链技术和隐私计算），能够提供更安全、透明数据管理解决方案。

六、结论

本文对智慧城市项目建设中的数据共享与数据安全问题进行了研究分析，笔者认为在智慧城市项目建设中可以从六个方面加以解决，并重点介绍了在组织和技术两个方面的创新型解决方案，对智慧城市项目建设具有一定的参考价值。

参考文献：

[1]郑崇明，高梁.数据共享、数据风险与智慧城市的平台选择——基于深圳市S区的实证研究[J].理论与改革，2023（03）：94-107.

[2]肖丽萍.大数据下智慧城市数据共享与安全的研究——以吉安市为例[J].信息系统工程，2018（12）：78.

[3]邹志威.国有企业参与智慧城市数据协同治理研究[D].武汉大学，2022.

[4]李凤华，李晖，贾焰等.隐私计算研究范畴及发展趋势[J].通信学报，2016，37（04）：1-11.

[5]李启飞.面向隐私保护的多方联合学习方法研究[D].哈尔滨工业大学，2020.