法，使系统能够根据用户在产量、资源投入与人力成本等方面的优先级设定，输出最具适应性的管理方案。

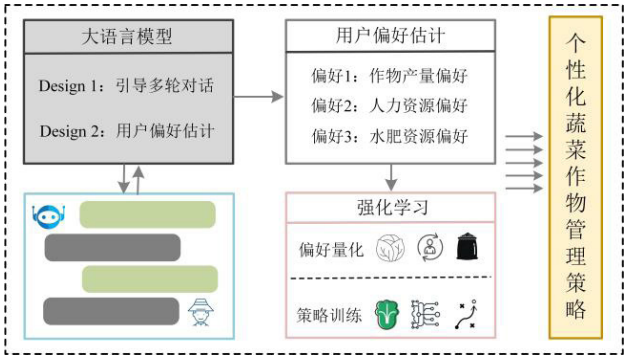

图 2 基于 LLM 的个性化蔬菜作物管理方法结构

4 嘉霖农科智链平台的特色与创新突破

4.1 技术融合创新

多元技术协同整合：本平台实现了人工智能与物联网、大数据、区块链等现代信息技术的有机结合，构建了完整的智慧农业生态系统。实践应用中，借助物联网终端完成农田信息采集，利用大数据平台进行信息存储与处理，通过人工智能技术生成决策建议，并运用区块链保障信息真实可靠，形成了农业生产全过程的数字化管控能力。

自主算法模型研发：针对农业应用场景的特殊性，研发团队自主构建了适配农业领域的机器学习算法与深度神经网络模型。结合农业数据的时空特性与业务需求对模型进行专门优化，显著提升了数据处理效能与决策精准度。以作物病害预警模型为例，其在多变环境下的识别精度较常规模型提升 10-15 个百分点。

全流程业务覆盖：平台服务范围贯穿农业生产的前、中、后全周期，包含农资采购、种植管理、加工储运及市场销售等核心环节，为产业链各方提供综合性服务支持，有效促进了农业各环节的协调发展。

信息互通与业务协同：平台消除了传统农业中的信息壁垒，实现了产业链各节点数据的实时互通。参与者可基于平台数据开展协同规划，如农资企业依据种植计划调整供货安排，加工企业根据产量品质制定生产方案。

4.2 基于数据的决策辅助

大规模农业数据处理：平台具备收集和存储海量农业数据的能力，运用智能分析技术深入挖掘数据价值，为使用者提供可靠的决策依据。例如，通过对市场行情数据的分析预测农产品价格走向，预测准确度超过 80%，有效指导生产主体制定产销计划。

差异化决策服务：平台根据用户类型和业务特征提供针对性的决策支持。面向规模化农业企业，可定制供应链优化方案；针对个体农户，则提供简明实用的种植管理建议，满足不同层次用户的需求。

5 现存问题与应对方案

5.1 技术难点及解决途径

数据质量与安全保障：农业数据来源多样，采集过程中易出现信息不全、记录错误等问题，同时存在数据泄露风险。为此，平台构建了完整的数据清洗与验证流程，实施标准化处理；并采用加密传输、权限管理等技术建立防护体系，如运用区块链存储关键数据确保不可篡改，通过多层加密保障数据传输与存储安全。

智能算法性能优化：农业生产环境的复杂性对算法适应性提出更高要求。平台通过扩展训练样本规模、改进模型架构，并结合实际应用效果持续优化算法表现。例如，定期更新病害图像库，完善识别模型训练集，提升对新型病虫害的检测能力。

参考文献

[1] 姜京池，闫莲，刘劼。基于精准知识筛选及知识协同生成的农业大语言模型 [J]. 智慧农业 (中英文),2025,7 (1).

[2] 金宁，郭宇峰，韩晓东，等。基于迁移学习的农业短文本语义相似度计算方法 [J]. 智慧农业 (中英文),2025,7 (1):33 - 43

[3] 刘喜永，纪伟娟，顾孔平. 农产品运营运营与营销内容研究 [C]. 农作物世界研讨会论文集，2020.

[4] 姚刚，王露，内容电商运营[M]. 北京：人民邮电出版社, 2021

 DOI: https://doi.org/10.12345/bdai.v6i6.34066

Research on Data Security and Privacy Protection in the Informatization of Government Data

Taiwen Xiao

Digital Government Operation Center, Haizhu District, Guangzhou, Guangdong , 510000, China

Abstract

The informatization of government data is crucial to improving government governance efficiency, but the accompanying issues of data security and privacy protection have become systemic challenges related to national security, citizen rights, and government credibility. Existing research and practice mostly focus on a single technology or management measure, which is difficult to deal with compound risks in the entire life cycle. This article introduces the concept of "Resilient Governance" and builds a "three-dimensional dynamic grading-dual-track technology integration-multiple collaborative co-governance" (3D-2T-MC) collaborative framework for the full life cycle of government data. Through dynamic compliance, technology integration and social co-governance, this framework provides a theoretically forward-looking and practical solution to solve the "impossible triangle" of data utilization and security protection.

Keywords

Government data security; privacy protection; resilient governance; zero trust architecture; privacy-enhanced computing; data classification and classification; collaborative framework

政务数据信息化中数据安全与隐私保护研究

萧太文

广州市海珠区数字政府运营中心，中国·广东 广州 510000

摘　要

政务数据信息化对提升政府治理效能至关重要，但伴随而来的数据安全与隐私保护问题已成为关乎国家安全、公民权利和政府公信力的系统性挑战。现有研究和实践多侧重于单一技术或管理措施，难以应对全生命周期中的复合型风险。本文引入“韧性治理”（Resilient Governance）理念，构建了面向政务数据全生命周期的“三维动态定级-双轨技术融合-多元协同共治”（3D-2T-MC）协同框架。该框架通过动态合规、技术融合和社会共治，提供了解决数据利用与安全保护“不可能三角”的理论前瞻性与实践操作性兼具的解决方案。

关键词

政务数据安全；隐私保护；韧性治理；零信任架构；隐私增强计算；数据分类分级；协同框架

1 引言

我国在数据利用效率与安全保障能力之间存在显著“鸿沟”。研究显示，我国政务数据共享率仅为经济合作与发展组织（OECD）成员国平均水平的 58%，表明数据孤岛现象依然严重，制约了数据要素价值的释放。与此形成鲜明对比的是，隐私侵权纠纷年均增长率高达 23%，反映出在数据流动与利用过程中，安全防护与隐私保护的短板日益凸显。这一“低共享率、高纠纷率”的悖论，深刻暴露了数据价值释放与安全保障之间存在的“不可能三角”矛盾——即难以同时实现数据的最大化利用、绝对安全与完全隐私。这一矛盾不仅威胁公民权益，更可能侵蚀政府公信力，阻碍数字化转型进程。在政务数据安全语境下，这意味着构建一个能够动态感知风险、自适应调整策略、整合多元力量、实现持续进化的安全生态。

本文旨在突破传统局限，系统分析政务数据在采集、传输、存储、处理、共享、销毁全生命周期中的复合型风险，借鉴国际先进治理经验，创新性地提出“三维动态定级 - 双轨技术融合 - 多元协同共治”（3D-2T-MC）韧性治理框架。该框架力图提供一个兼具理论前瞻性与实践操作性的解决方案，为构建安全、可信、可持续的数字政府生态贡献新的治理路径。

2 政务数据全生命周期风险解构

政务数据安全并非单一环节的防护，而是一个贯穿于

【作者简介】萧太文（1988–），男，中国广东茂名人，硕士，工程师，从事计算机技术、网络工程、电子与通信工程研究。

数据从产生到消亡的全生命周期的系统工程。任何环节的疏漏都可能引发连锁反应，导致重大安全事件。本节将从技术、管理、法律三个维度，深入解构各阶段存在的复合型风险及其耦合机制。

2.1 技术脆弱性：系统性安全威胁的根源

技术是保障安全的基础，但技术本身的局限性与复杂性也构成了主要风险源。

云环境与系统异构带来的整合风险：政务云的普及极大提升了资源利用率与服务弹性，但多云、混合云环境下的数据传输与存储安全挑战加剧。不同部门、不同层级的系统在技术栈、数据格式、安全标准上存在差异，形成“数据烟囱”与“安全孤岛”，不仅阻碍了数据共享，更因接口复杂、协议多样而增加了攻击面。

接口与已知漏洞的暴露：API 作为数据共享与服务集成的关键通道，若缺乏严格的访问控制、频次限制与输入验证，极易成为攻击入口。某市健康宝系统因未对 API 实施访问频次控制，被黑客利用撞库攻击获取大量居民健康信息，即是典型例证。此外，对已知漏洞的疏于修补是重大隐患。某市社保查询系统未及时修复 Apache Log4j 远程代码执行漏洞，导致黑客成功植入勒索软件，造成了严重的公共服务中断与经济损失。

供应链安全盲区：政务系统大量依赖第三方软硬件产品与服务。某市智慧停车系统采用的第三方 SDK 在未经用户充分知情同意的情况下，违规持续采集车主行踪轨迹，最终导致数百万人的位置信息被非法转售，凸显了供应链安全管理的薄弱环节。

2.2 管理失能：内部威胁与流程缺陷的放大器

再先进的技术，若缺乏有效的管理，其防护能力将大打折扣。管理失能是导致数据泄露的最常见原因之一。

内部人员风险：研究表明，高达 34% 的数据泄露事件源于内部人员，包括操作失误、疏忽大意或蓄意的越权访问。权限管理不善是核心问题。某政务平台因未及时清理或严格限制测试账号的权限，导致测试人员可访问生产环境中的真实居民信息并被违规下载。

权限失控与滥用：最小权限原则在实践中常被忽视。某政务云平台运维人员拥有过高的数据库备份权限，且缺乏有效的操作审计与行为监控，使其得以将包含敏感信息的数据库备份复制至个人设备并在黑市交易，造成大规模数据泄露。

应急响应与溯源能力不足：面对突发安全事件，快速响应与精准溯源至关重要。尽管相关部门推动建立“熔断机制”要求短时间内启动处置，但复杂系统的漏洞定位与修复仍需时日，反映出应急流程、技术工具与专业人才储备的不足。

2.3 制度滞后：法规适配性与执行困境的制约

完善的法律制度是治理的基石，但法规的滞后性与执行中的模糊地带同样构成风险。

分类分级标准的静态化与僵化：相关条例确立了重要数据目录制度，但政务数据的敏感度是动态变化的。例如，某次人口普查的精确到门牌号的数据在普查期间属“机密”，但若干年后公开部分汇总数据时，其敏感度已大幅降低。现有的静态分类分级标准难以实现这种动态调整，导致“该放的放不开，该管的管不住”。

“公共利益例外”条款的边界模糊：在疫情防控等紧急状态下，政府可基于公共利益收集和使用个人信息。但紧急状态结束后，这些数据的保留期限、使用范围、是否可进行科研或商业分析，缺乏清晰的实施细则。这种法律灰色地带，既可能侵犯公民隐私，也可能因过度担忧合规风险而阻碍数据在公共治理中的后续价值挖掘。

3 国际比较与先进治理要素提炼

借鉴国际先进经验，是完善我国治理体系的重要途径。本节通过比较分析欧盟、美国、新加坡及我国的治理模式，提炼可资借鉴的先进治理要素。

表 1 国际政务数据保护模式比较

国家 / 地区	法律框架	技术特色	管理创新	启示性实践
欧盟	GDPR 统一规制，以“数据主体权利”为核心	隐私设计 (Privacy by Design)，将隐私保护内嵌于系统设计	数据保护官 (DPO) 强制设置，独立监督	法国 HealthDataHub 集中管理医疗数据，采用联合学习技术实现医院间协同分析，数据不出域
美国	联邦与州立法并存（如 CCPA），侧重行业自律与消费者保护	联邦政府推行 TIC3.0 可信互联网连接架构，强化边界与访问控制	FISMA 法案要求联邦机构实施持续监控（Continuous Monitoring）	2024 年联邦零信任战略，要求所有政府机构实施身份治理，最小权限访问覆盖率需达 90%
新加坡	PDPA 个人数据保护法，平衡创新与保护	国家数字身份 (NDI) 体系，实现安全便捷的身份认证	设立数据信任中心（Data Trust Centre），由可信第三方托管高敏数据	“技术中立”原则：允许政府基于公共利益经法院授权访问加密数据，并需事后公示
中国	以《网络安全法》《数据安全法》《个人信息保护法》为基石，辅以《条例》	政务云全面推行网络安全等级保护 2.0（等保 2.0）	推行数据分类分级制度，探索数据要素市场化	上海“一网通办”示范：技术（联邦学习）、保险（责任险）、监管（月审季评年检）结合