

数字文旅专业系列教材 · 教学课件

智慧旅游系统架构设计与实践

第9章 韧性与安全治理层（R）——数据安全与隐私保护

授课对象：安顺学院旅游管理学院 · 旅游管理专业本科生

主讲：祝刚

本章导览

- 9.1 智慧旅游安全治理体系
- 9.2 数据安全和隐私保护
- 9.3 区块链赋能旅游信任机制
- 9.4 系统容灾与弹性伸缩

- 识记：智慧旅游安全治理体系的构成要素
- 理解：数据安全与隐私保护的技术方案与法律要求
- 应用：设计智慧旅游系统的安全治理架构
- 分析：分析区块链在旅游信任机制中的应用模式
- 评价：评估系统容灾与弹性伸缩方案的有效性
- 创造：设计面向多中心治理的智慧旅游安全方案

- Masseno 和 Santos （2018）在研究智慧旅游目的地的隐私风险时指出 [1]，" 由游客产生并在智慧旅游环境中处理的数据大多涉及来自社交网络、智能应用、
- 无处不在的传感器等多种来源的个人数据 "。
- 欧盟 GDPR 的实施迫使智慧旅游系统在架构层面内嵌隐私保护机制（Privacy by Design），这一要求深刻影响了欧洲智慧旅游系统架构的设计取向。

01

9.1 智慧旅游安全治理体系

9.1.1 韧性架构的概念与设计原则

- 韧性架构（ Resilient Architecture ）是指系统在面对故障、攻击或异常负载时能够保持核心功能可用、并在事后快速恢复的架构设计。

9.1.1 韧性架构的概念与设计原则

- 韧性架构的设计原则包括：冗余部署（关键组件多实例运行）、故障隔离（一个组件故障不影响其他组件）、优雅降级（在部分功能不可用时仍提供基本服务）和自动恢复（无需人工干预的故障恢复）。

9.1.2 安全治理层在 S.M.A.R.T. 框架中的定位

- 安全治理层（R）是 S.M.A.R.T. 框架的创新维度——传统架构模型中安全治理往往作为附加组件，而 S.M.A.R.T. 将其提升为独立维度。

9.1.2 安全治理层在 S.M.A.R.T. 框架中的定位

- 这反映了智慧旅游系统从纯技术系统向社会 - 技术系统演进的趋势。

9.1.2 安全治理层在 S.M.A.R.T. 框架中的定位

- 王琼阁（2025）在分析智慧旅游数据安全时指出 [2]，" 大数据技术的广泛应用带来的数据汇聚虽为旅游服务的优化提供了机遇，但也带来了安全上的挑战 "。

9.1.3 多中心治理机制

- Yu 和 Wang （2022）提出的多中心治理机制 [3] 为智慧旅游安全治理提供了理论框架。多中心治理打破传统的自上而下管理模式，形成政府监管、企业自律、社会监督和游客参与的多元协同治理结构。

- ◆ 9.1.1 韧性架构的概念与设计原则
 - 韧性架构（Resilient Architecture）是指系统在面对故障、攻击或异常负载时能够保持核心功能可用、并在事
 - 韧性架构的设计原则包括：冗余部署（关键组件多实例运行）、故障隔离（一个组件故障不影响其他组件）、优雅降级（在部分功能不可
- ◆ 9.1.2 安全治理层在 S.M.A.R.T. 框架中的定位
 - 安全治理层（R）是 S.M.A.R.T. 框架的创新维度——传统架构模型中安全治理往往作为附加组件，而 S.M.A.R.T. 将
 - 这反映了智慧旅游系统从纯技术系统向社会 - 技术系统演进的趋势。

02

9.2 数据安全性与隐私保护

9.2.1 智慧旅游数据安全风险识别

- 智慧旅游系统面临的数据安全风险包括：数据泄露（黑客攻击或内部人员窃取）、数据篡改（恶意修改旅游数据如虚假评价）、

9.2.1 智慧旅游数据安全风险识别

- 数据滥用（超出授权范围使用个人数据）和数据丢失（系统故障或自然灾害导致数据损毁）。

9.2.2 个人信息保护的法律框架

- 中国的数据安全法律体系以《网络安全法》《数据安全法》《个人信息保护法》三大法律为支柱。《个人信息保护法》要求个人信息处理遵循 " 最小必要 " 原则，GDPR 要求 " 默认隐私 " 设计。

9.2.2 个人信息保护的法律框架

- 这些法规要求数据平台层（M）在设计时就限定数据采集范围。

9.2.3 隐私保护技术

- 差分隐私。在数据查询结果中添加受控噪声，使攻击者无法推断任何特定个体的信息。

9.2.3 隐私保护技术

- 联邦学习。多个数据持有方在不共享原始数据的情况下联合训练 AI 模型，数据 " 可用不可见 "。

9.2.3 隐私保护技术

- 同态加密。允许在加密数据上直接进行计算，无需解密即可获得计算结果。

9.2.4 数据全生命周期安全管理

- 数据全生命周期包括采集、传输、存储、处理、共享和销毁六个阶段。

9.2.4 数据全生命周期安全管理

- 每个阶段都有特定的安全要求：采集阶段需获告知同意，传输阶段需加密通信，存储阶段需加密存储和访问控制，处理阶段需数据脱敏，共享阶段需授权管理，销毁阶段需不可恢复删除。

- ◆ 9.2.1 智慧旅游数据安全风险识别

- 智慧旅游系统面临的数据安全风险包括：数据泄露（黑客攻击或内部人员窃取）、数据篡改（恶意修改旅游数据如虚假评价）、数据滥用（超出授权范围使用个人数据）和数据丢失（系统故障或自然灾害导致数据损毁）。

- ◆ 9.2.2 个人信息保护的法律框架

- 中国的数据安全法律体系以《网络安全法》《数据安全法》《个人信息保护法》三大法律为支柱。《个人信息保护法》要求个人信息处理
- 这些法规要求数据平台层（M）在设计时就限定数据采集范围。

03

9.3 区块链赋能旅游信任机制

9.3.1 区块链技术在旅游中的应用综述

- Rana 等（2022）的系统性文献综述全面梳理了区块链技术在旅游行业的应用 [4]。

9.3.1 区块链技术在旅游中的应用综述

- 明庆忠和韦俊峰（2021）探讨了“区块链+”赋能智慧旅游高质量发展的路径[5]，指出推动区块链技术与智慧旅游融合应用有利于提升智慧旅游公共服务平台效能。

9.3.2 旅游信用管理系统

- 区块链的不可篡改特性适合构建旅游信用管理系统——游客的评价、消费和行为记录上链后无法被篡改，为旅游信用评价提供了可信数据基础。

9.3.3 去中心化旅游服务平台

- Zhang 等（2020）研究了区块链旅游服务平台的互操作机制 [6]，探讨了去中心化旅游平台的架构设计。去中心化平台消除了中间商，使游客和服务提供者直接交易。

9.3.4 智能合约与旅游交易

- 智能合约可以自动执行旅游交易——当游客到达酒店时自动触发付款，当航班延误时自动触发理赔。这种自动化降低了交易成本和纠纷概率。

04

9.4 系统容灾与弹性伸缩

9.4.1 高可用架构设计

- 高可用架构通过冗余部署和故障自动转移实现系统的持续可用。智慧旅游系统的核心服务（如票务、应急）通常要求 99.99% 以上的可用性，即年停机时间不超过 52.6 分钟。

9.4.2 异地多活与容灾恢复

- 异地多活是在不同地理位置部署多个活跃数据中心，任一数据中心故障时其他中心可以接管服务。肖荣和高全亮（2019）的智慧景区平台 [7] 通过云平台的跨可用区部署实现了容灾能力。

9.4.3 弹性伸缩与自动扩容

- 微服务架构支持按服务的负载独立扩缩容。在节假日大客流场景下，票务和导览服务可以自动扩容，而营销和分析服务可以缩容以释放资源。

- 韧性与安全治理层（R）是 S.M.A.R.T. 框架的安全基石。
- 本章阐述了韧性架构的设计原则和多中心治理机制，详细介绍了数据安全风险识别、法律框架和隐私保护技术（差分隐私、联邦学习、同态加密），分析了区块链在旅游信用管理、
- 去中心化平台和智能合约中的应用，讨论了高可用架构、异地多活和弹性伸缩等容灾方案。

- （识记）数据全生命周期的六个阶段及各阶段安全要求是什么？
- （理解）比较差分隐私、联邦学习和同态加密三种隐私保护技术的原理。
- （应用）为一个智慧旅游平台设计数据安全治理架构方案。
- （分析）分析区块链技术如何解决旅游行业的信任问题。
- （评价）评估多中心治理机制在智慧旅游安全治理中的适用性。
- （创造）设计一个融合区块链和联邦学习的旅游数据安全共享方案。

- [1] Masseno M D, Santos C. Smart Tourism Destinations Privacy Risks on Data Prot
- [2] 王琼阁 . 智慧旅游数据安全与隐私保护：问题根源、用户意识觉醒及综合应对策略 [J]. 万方数据 , 2025.
- [3] Yu Y, Wang H. Study on the construction of smart tourism ecosystem and polyc
- [4] Rana R L, et al. The Impact of Blockchain Technology Adoption on Tourism Ind
- [5] 明庆忠 , 韦俊峰 . " 区块链 +" 赋能智慧旅游高质量发展探析 [J]. 维普 , 2021.
- [6] Zhang L, et al. Interworking Mechanism of Blockchain Platforms for Secure To

谢谢聆听 · 下章再见

安顺学院旅游管理学院 · 数字文旅专业系列教材