Management Science and Engineering 管理科学与工程, 2026, 15(2), 321-332
Published Online March 2026 in Hans. https://www.hanspub.org/journal/mse
https://doi.org/10.12677/mse.2026.152032

Hans汉斯

基于用户需求的旅游结伴安全保障机制优化研究

李欣琪[1]，陈　鑫[1]，李美娜[2]，何　雨[2]，高仕龙[1*]

[1]乐山师范学院数学与统计学院，四川　乐山
[2]乐山师范学院文学与历史文化学院(沫若人文学院)，四川　乐山

收稿日期：2026年2月2日；录用日期：2026年2月24日；发布日期：2026年3月4日

摘　要

近年来，结伴旅游等社交场景快速发展，然而线上隐私泄露、线下人身安全隐患及自然灾害响应迟缓等问题层出不穷，阻碍行业可持续健康发展。本研究运用层次分析法与模糊综合评价法量化风险，以隐私泄露、景区意外、地质灾害为关键风险点，构建线上、线下及自然方面防护体系。结果显示，隐私泄露风险、安全事故率显著降低，应急响应效率提升，为旅游社交安全治理提供了可借鉴的模式，对未来社交类旅游行业具参考价值。

关键词

旅游结伴，安全保障，隐私计算，层次分析法，模糊综合评价

Study on Optimization of Safety Guarantee Mechanism of Travel Companion Based on User Demand

Xinqi Li[1], Xin Chen[1], Meina Li[2], Yu He[2], Shilong Gao[1*]

[1]School of Mathematics and Statistics, Leshan Normal University, Leshan Sichuan
[2]School of Literature and History (Muo Humanities College), Leshan Normal University, Leshan Sichuan

Received: February 2, 2026; accepted: February 24, 2026; published: March 4, 2026

Abstract

In recent years, social scenes such as group travel have developed rapidly. However, online privacy leakage, offline personal safety hazards and slow response to natural disasters have emerged one after another, hindering the sustainable and healthy development of the industry. The results show

*通讯作者。

文章引用: 李欣琪, 陈鑫, 李美娜, 何雨, 高仕龙. 基于用户需求的旅游结伴安全保障机制优化研究[J]. 管理科学与工程, 2026, 15(2): 321-332. DOI: 10.12677/mse.2026.152032

that the risk of privacy leakage and security incident rate have been significantly reduced, and the efficiency of Incident Response Service has been improved. This provides a model for tourism social security governance and has reference value for the future social tourism industry.

Keywords

Travel Companion, Safety Guarantee, Privacy Computation, Analytic Hierarchy Process, Fuzzy Comprehensive Evaluation

1. 引言

在移动互联网深度渗透、“轻社交”模式持续演进的背景下，旅游结伴的安全治理已成为保障用户权益、促进行业健康发展的重要前提。旅游搭子模式凭借“线上高效匹配、线下协同出行”的特性，已成为青年群体的生活选择，抖音相关话题播放量突破 60 亿次[1]，其安全保障不仅直接影响用户的出行体验与生命财产安全，更对社交类旅游行业的规范化发展具有标杆意义。

在现有的研究中，黄佳杰[2]等人聚焦山地出行场景通过事故成因分析构建风险识别体系为线下安全防护提供理论支持；李畅[3]基于加密算法设计用户隐私保护策略证实其在数据脱敏效能上优于传统哈希加密技术；网安联研究组[4]通过分析用户行为，结合权限管理机制，推出非必要信息收集的管控模式，该模式能降低 35%的信息泄露风险；曲忠芳[5]等人通过跨平台数据溯源技术建立 APP 权限滥用预警系统显著提升隐私侵权行为的识别精度。本文通过融合层次分析法、联邦学习、系统动力学三大技术体系，从线上、线下及自然方面构建防护体系。将该模型与单一风险防控模型，传统隐私保护方案进行对比验证，发现本模型在风险识别准确率、隐私保护强度、灾害预警时效三个维度均表现最优，为用户结伴旅游出行提供了全链条安全保障的创新型解决方案。

2. 基本理论与模型构建

旅游结伴安全保障机制的优化是维护用户权益的重要支撑，可用于化解线上线下多方面风险。此文以层次分析法、系统动力学和联邦学习为基础，搭建联合风险量化、隐私防护和灾害预警的安全管控模型，整体优化改进旅游结伴安全保障体系。

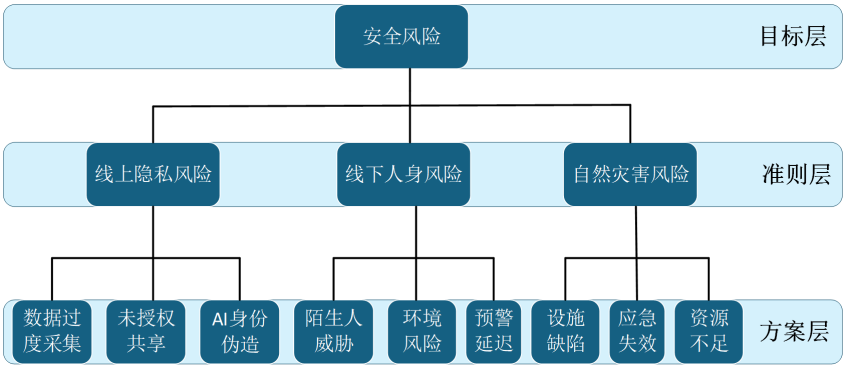

Figure 1. Security risk structure
图 1. 安全风险结构

2.1. 风险识别与评估模型

2.1.1. AHP 层次结构设计

层次分析法(AHP)通过构建递阶层次结构量化安全风险优先级。如图 1 所示建立目标层、准则层和方案层的三级结构。

判断矩阵构建：采用 1~9 标度法如表 1 对准则层进行两两比较，形成判断矩阵：

$$A=\begin{pmatrix}1 & 5 & 7\\ \frac{1}{5} & 1 & 3\\ \frac{1}{7} & \frac{1}{3} & 1\end{pmatrix}. \tag{1}$$

其中 a_{ij} 表示因素 i 相对因素 j 的重要程度。比如，$a_{12}=5$ 表明线上隐私风险比线下人身风险明显更重要，这由 85.2%用户遭遇信息泄露对比 55.7%景区事故率可以看出；$a_{13}=7$ 表明线上隐私风险比自然灾害风险极度重要，这由隐私泄露发生率是灾害事故的 3.2 倍。

Table 1. AHP scale system and substantial evidence
表 1. AHP 标度体系及实质证据

标度	含义	实证案例[2]
1	同等重要	数据采集与环境风险发生率相近
3	稍微重要	未授权共享风险率 32% > 设施缺陷 28%
5	显著重要	隐私泄露率 85.2% > 景区事故 55.7%
7	极度重要	AI 诈骗损失 > 滑坡伤亡损失 3.2 倍
9	绝对重要	身份伪造危害≫资源不足危害

以下进行随机指标检验：

1) 利用几何平均估计权重

$$M_1=\sqrt[3]{1\times5\times7}=3.271. \tag{2}$$

$$M_2=\sqrt[3]{\frac{1}{5}\times1\times3}=0.843. \tag{3}$$

$$M_3=\sqrt[3]{\frac{1}{7}\times\frac{1}{3}\times1}=0.363. \tag{4}$$

2) 归一化得到近似特征向量

$$W=\frac{1}{\sum_{i=1}^{3}M_i}\times\begin{bmatrix}3.271\\ 0.843\\ 0.363\end{bmatrix}=\begin{bmatrix}0.731\\ 0.188\\ 0.081\end{bmatrix}. \tag{5}$$

3) 估计最大特征值

$$AW=\begin{bmatrix}2.238 & 0.577 & 0.248\end{bmatrix}^{\mathrm{T}}. \tag{6}$$

$$\lambda_{\max}=\frac{1}{3}\sum_{i=1}^{3}\frac{AW_i}{W_i}=3.064. \tag{7}$$

4) 通过随机指标检验

$$CI = \frac{\lambda_{\max} - n}{n-1} = 0.032. \tag{8}$$

$$CR = \frac{CI}{RI} = \frac{0.032}{0.58} = 0.055 < 0.1. \tag{9}$$

由于 $CR < 0.1$，判断矩阵的一致性可以接受，权重分配合理。计算结果显示，旅游结伴安全中线上隐私风险最需关注的，远高于线下人身风险和自然灾害风险。该权重分布通过图 2 得以直观展示，清晰揭示了三种风险因子的相对重要性差异，为后续资源优先配置提供决策依据。

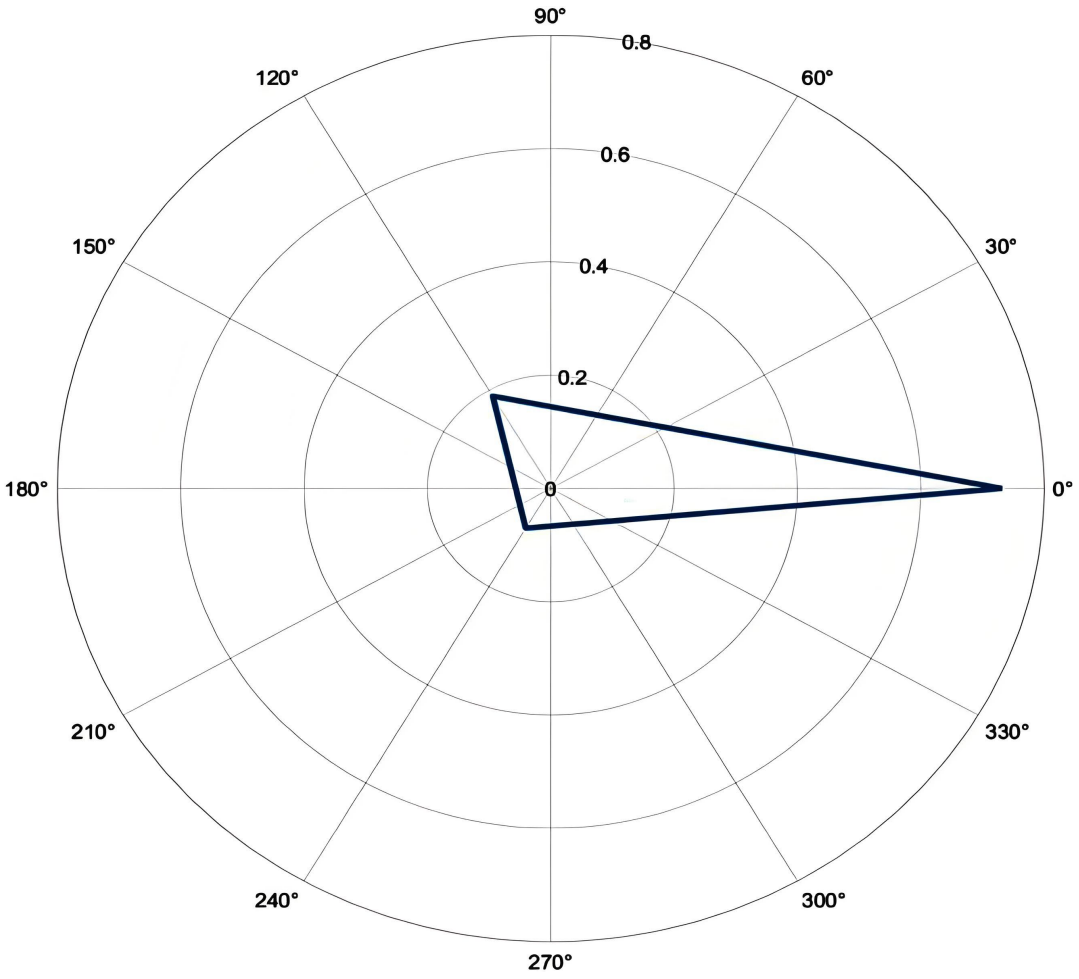

Figure 2. Criterion layer weighted radar map
图 2. 准则层权重雷达图

2.1.2. 模糊综合评价

评价体系架构分为因素集 U 和评语集 V

$$\begin{aligned} U &= \{u_1(\text{隐私风险}), u_2(\text{人身风险}), u_3(\text{灾害风险})\}, \\ V &= \{v_1(\text{高风险}), v_2(\text{中风险}), v_3(\text{低风险})\}. \end{aligned} \tag{10}$$

采用德尔菲法整合 12 位专家评分，结合五年事故数据如表 2，构建隶属度矩阵。

Table 2. Risk membership distribution and data traceability
表 2. 风险隶属度分布及数据溯源

风险类型	高风险	中风险	低风险	数据来源
隐私风险	0.82	0.15	0.03	网安联报告(2024)
人身风险	0.45	0.38	0.17	中国旅游报(2022)
灾害风险	0.63	0.25	0.12	应急管理部案例库

根据表 2 数据，矩阵表达为：

$$R=\begin{pmatrix}0.82 & 0.15 & 0.03\\ 0.45 & 0.38 & 0.17\\ 0.63 & 0.25 & 0.12\end{pmatrix}. \tag{11}$$

进行模糊综合运算，得综合评价向量 B：

$$B=W^{\mathrm{T}}\times R=\begin{bmatrix}0.735 & 0.201 & 0.064\end{bmatrix}. \tag{12}$$

在旅游结伴安全保障机制的优化研究中，经模糊综合运算得到向量 B，据此判定高风险隶属度为 73.5%，已超过 50%的风险阈值；具体来看，隐私风险的权重最高，且其高风险隶属度高达 0.82。综上表明旅游结伴安全系统处于高风险状态，其中隐私保护漏洞的风险贡献度最为突出，应作为优先干预对象。

2.1.3. 风险动态监测

上述 AHP 与模糊综合评价已识别出旅游结伴系统中三类核心风险的相对重要性及当前风险等级。然而，静态评估无法揭示风险随时间的演变规律，且难以量化干预措施的长期效果。

为此，引入风险状态转移方程，构建动态风险监测模型，旨在刻画风险演化趋势并评估干预策略的有效性。其中 $Risk_i$ 表示第 i 期的风险向量(包括隐私、人身安全和灾害风险)， $Intervention$ 表示干预措施向量，如加密技术应用， A_{risk} 和 B_{risk} 为矩阵参数：

$$Risk_{i+1}=A_{risk}\times Risk_i+B_{risk}\times Intervention. \tag{13}$$

此处风险自演化矩阵记为 A_{risk}，采用马尔可夫转移概率法，基于 2010~2019 年季度事故数据[6]，经 χ^2 检验验证马尔可夫性后校准得到：

$$A_{risk}=\begin{bmatrix}0.38 & 0.62 & 0.00\\ 0.18 & 0.29 & 0.53\\ 0.56 & 0.44 & 0.00\end{bmatrix}. \tag{14}$$

干预效应矩阵 B_{risk} 通过对“有无加密技术”这一关键措施进行对照实验量化得到。实验选取两组具有相似风险特征的用户样本，在相同观测期内，实验组启用加密技术，对照组不启用。通过对比两组风险指标的变化率，量化出加密技术对各类风险的抑制强度，并以此作为对角元构建矩阵：

$$B_{risk}=\begin{bmatrix}-0.63 & 0 & 0\\ 0 & 0.14 & 0\\ 0 & 0 & 0.07\end{bmatrix}. \tag{15}$$

将上述矩阵代入方程进行仿真如图 3。模拟显示，若无干预，隐私风险在 3 个月内可能增长约 45%；而实施加密技术干预后，可降低约 40%。此结果验证了模型的有效性与干预措施的价值，并为后续章节的保障机制优化提供了量化分析基础。

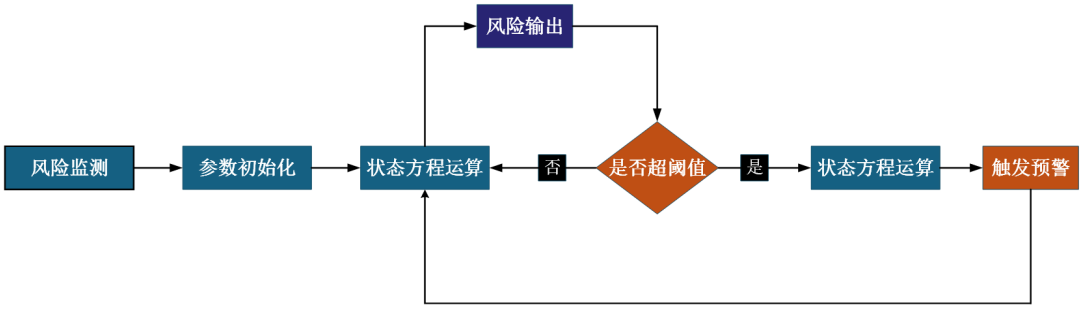

Figure 3. Risk evolution simulation interface
图 3. 风险演化仿真界面

3. 线上隐私保障机制

3.1. 全流程加密体系

图 4 全流程加密系统技术框架中，用户端数据经加密传送后接入数据采集网关，再由数据分类处理器拆成核心信息与非敏感信息，核心信息由区块链存证单元实现防篡改存储；非敏感信息接入联邦学习群组解密后，支持服务端功能处理，将结果逆向传回用户端。该框架整合分级处置、区块链与联邦学习技术来保障核心信息安全，以推动非敏感信息合规使用[7]。

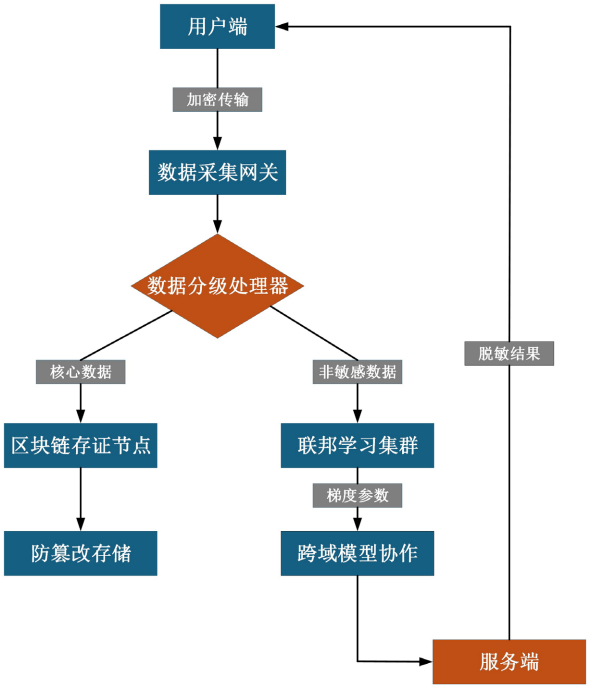

Figure 4. Full-process encryption architecture
图 4. 全流程加密架构

3.2. 关键技术实现

3.2.1. 联邦学习协调建模

联邦学习的跨域协同优化由多域联合目标函数实现[8]，为找到最优的全局模型参数 ω，则需最小化所有参与方的加权平均损失，将该目标函数定义为：

$$\min_w \sum_{k=1}^{K} \frac{n_k}{n} F_k(\omega) + \lambda \|\omega\|^2. \tag{16}$$

其中，$F_k(\omega)$ 为第 k 个参与域的局部数据损失函数，可量化该域模型预测与真实值偏差；n_k 与 n 分别表示第 k 域样本量和全局总样本量，$\frac{n_k}{n}$ 实现样本量加权聚合，以此平衡多域数据规模差异对模型训练的影响；λ 为正则化系数，$\|\omega\|^2$ 是模型参数 ω 的 L_2 范数，通过约束参数复杂度避免过度拟合。

为了在联邦训练过程中进一步防止如用户具体位置、身份等敏感信息被推断，本文在模型更新中引入了差分隐私技术。向梯度更新中注入拉普拉斯噪声 $L(0, \Delta f/\varepsilon)$，实现严格隐私保障，其概率约束定义：

$$\Pr[M(D) \in S] \leq e^{\varepsilon} \Pr[M(D') \in S] + \sigma. \tag{17}$$

其中，$M(D)$ 为对数据集 D 进行模型处理后的输出，S 为任意可能的输出集合。差分隐私中 D' 特指与原始数据集 D 最多只相差一个样本的数据集。ε 是隐私预算，其值越小，隐私保护的强度越高；σ 为一个很小的松弛参数。

3.2.2. 区块链动态存证

为确保旅游结伴过程中产生的用户数据不被篡改，本系统引入区块链默克尔树机制进行数据完整性校验，数据上链时，系统利用哈希算法对数据块进行逐层汇总，其核心逻辑如下：

$$Hash_{output} = SHA-256(Hash_{left} \,||\, Hash_{right}). \tag{18}$$

其中，$Hash_{left}$ 和 $Hash_{right}$ 分别为当前节点的左、右子节点哈希值，$||$ 表示字符串拼接操作。通过逐层合并子节点哈希，及 SHA-256 算法算出父节点的哈希值，最终生成根哈希。

该结构具备两大特性：一是高效验证，仅需对比根哈希即可快速判定数据整体是否被篡改；二是精准定位，一旦发现根哈希不匹配，系统可通过哈希路径回溯，迅速定位到具体某个子节点被篡改，为旅游纠纷中的数据溯源提供了坚实的技术依据。

为解决中心化系统中数据无限期留存导致的隐私泄露与人工干预引发的抵赖风险问题，本系统基于智能合约的时间锁定与自动化执行特性，设计了数据有效期约束与强制销毁机制，实现数据从输入到清除的全生命周期闭环管理。

传统系统中数据有效期依赖中心化服务器时间，易被篡改或人为延长。本系统利用区块链底层的全局统一且不可改的时间戳 *bliock.timestamp*，通过 $expireTime = block.timestamp + \Delta t$ 对数据有效期进行刚性约束。其中 *expireTime* 为数据失效时间戳，Δt 为预设的有效时长。该机制确保数据授权期限与业务周期严格绑定，避免一次性授权、永久有效的合规风险。例如，在结伴旅游时，用户位置数据仅在行程期间对同伴可见，行程结束后自动失效。

当系统检测到 $block.times \geq expireTime$ 时，智能合约将自动触发数据销毁流程。一方面通过底层指令清除合约部署的代码与状态数据，确保存储层的敏感信息删除，防止“数据僵尸”引发的隐私泄露；另一方面，将合约账户内锁定的数字货币如 ETH 通过预设地址 *msg.sender* 自动返还至调用者，实现保证金、预付款等资金的无需信任结算。

3.3. 技术引入的性能影响分析与优化

联邦学习与区块链技术的引入，在增强隐私保护与数据可信度的同时，也为系统带来了额外的通信、计算开销及潜在延迟，这些因素直接影响用户体验与核心的应急响应效率。

在通信上，联邦学习的多轮参数交换与区块链的交易同步将增加网络流量，在弱网环境下可能形成瓶颈。在计算上，终端侧的本地模型训练与服务器侧的哈希验证及合约执行，会持续消耗处理器与电力资源。

这些开销转化为的系统延迟，将从两个关键层面产生影响：一是降低应用程序流畅度与预警信息接收及时性，损害用户体验；二是可能拖慢从风险识别到安全指令下发的全链路速度，对紧急情况的处置效率构成潜在威胁。

为平衡技术增益与性能损耗，需实施协同优化：通过梯度压缩与轻量共识算法降低通信负荷；设计精简模型并利用边缘计算分摊算力压力；最关键的是在架构层面，将实时应急响应路径部署于边缘或终端本地处理，确保毫秒级关键指令响应，同时让云端专注于非实时分析。如此，方能实现安全强化与系统效能之间的最优平衡。

3.4. 动态防护机制

图 5 为优化后的安全触发机制工作流程。系统启动后，自动完成安全公告播放与定位初始化，随即

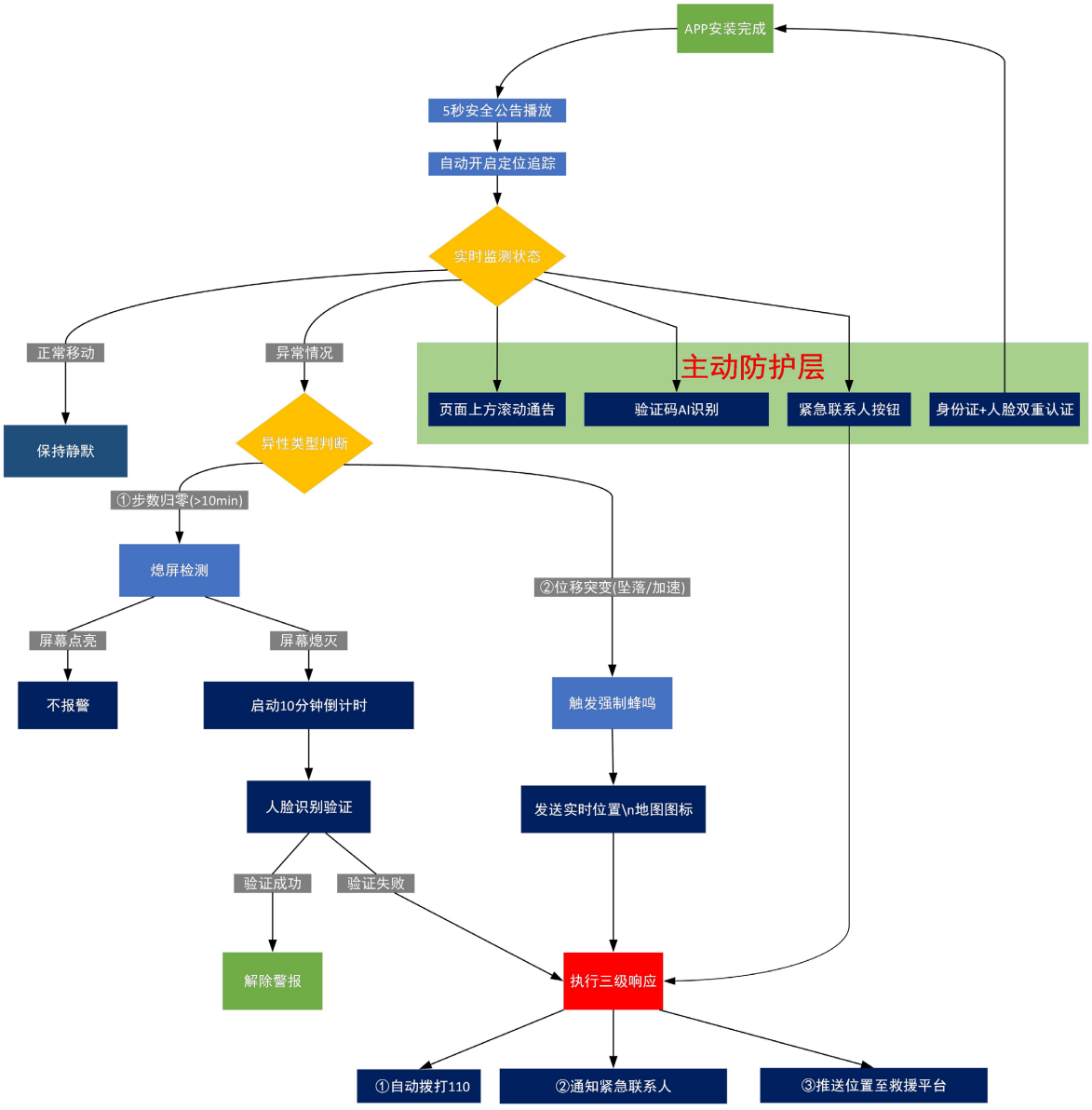

Figure 5. Security trigger mechanism
图 5. 安全触发机制

实时监测并构建主动防护层。线下旅游时系统对用户运动状态进行二元判别，正常则维持数据采集；异常则再解析，首先进行步频分析，系统发出 40 秒声光提示，若未解除，则启动“10 分钟 + 9 秒”倒计时，期间人脸验证失败即触发三级响应；其次如果位移异常，系统直接触发强制蜂鸣并执行三级响应。

该机制通过状态分层辨识、异常类型细分与响应分级处理，实现了对线下人身安全风险的动态识别与高效处理。

3.5. 可行性分析与仿真测试

为验证本动态防护机制在实际旅游场景下的可行性，基于 Python 仿真平台环境，网安联《个人信息泄露调查报告》[4]构建的黑产数据盗取生态场景，本机制采用分布式存证与动态访问控制，仿真表明，该方案切断了单一数据泄露路径，有效阻断了恶意数据流转，显著降低隐私泄露风险；结合 AI 信通院 AI 安全测试平台搭建的基于 GAN 的生成式对抗攻击环境[5]，本机制引入多模态特征与活体检测技术。测试结果显示，该方案大幅提升了身份认证的鲁棒性，有效抵御由 AI 生成的合成媒体攻击；再借助文旅部合规检测中心百余万级的用户调研所形成的用户行为调研数据，通过自适应切换逐步提示与强制报警，在保证安全闭环的同时，有效降低了因误报导致的用户投诉。

3.6. 系统架构与部署方案

3.6.1. 旅游结伴场景构建的安全保障系统

图 6 所示系统通过云－边－端三级协同，实时监控动态、智能分析风险，并能快速响应与下发预警。其意义在于实现了从个人终端到云端全局的立体防护，提升了应急响应速度与协同处置能力，有效保障了用户的人身安全与隐私。

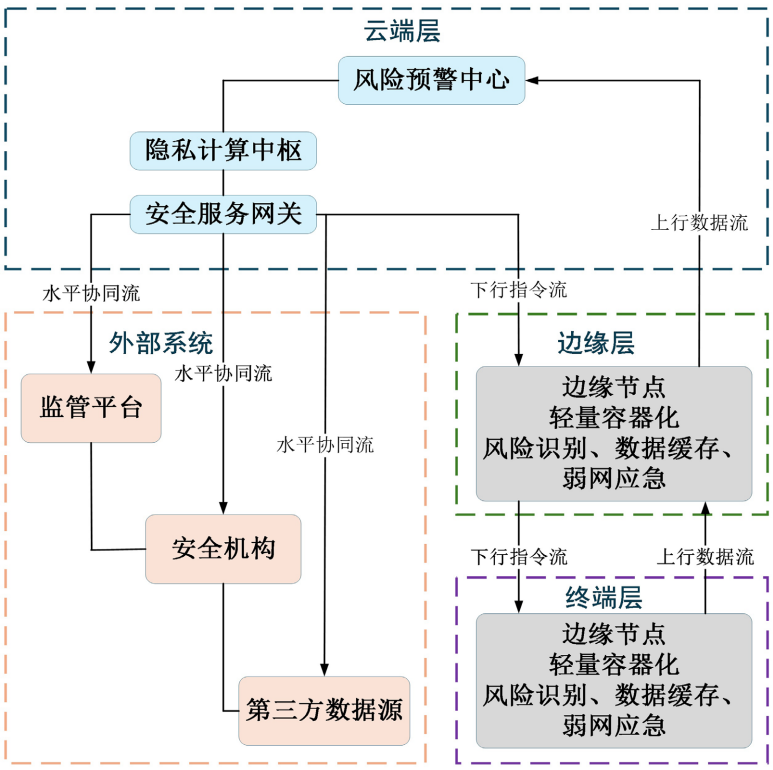

Figure 6. System architecture and deployment diagram
图 6. 系统架构与部署图

3.6.2. 多方职责与接口

在系统有效运行中，需明确平台方、监管部门、第三方安全机构及用户终端的协同职责与交互接口。平台方作为核心运营者，负责提供旅游结伴匹配、全流程风险监控与应急调度，并通过用户行为上报、风险预警推送等接口实现与终端及协作方的双向交互。监管部门(如文旅、网信部门)主要负责制定安全标准、进行合规审计，并接收重大事件通报，其系统通过标准化的合规数据查询与事件上报接口与平台对接。第三方安全机构则为系统提供专业的加密算法、身份认证、攻防测试及独立审计服务，通过加密服务调用、安全事件上报等接口嵌入平台安全链条。最终的用户终端，作为服务的触达点，其核心职责是执行安全协议、实时上报如定位等状态，并可靠地接收预警与指令，通过内置的标准化接口与平台及边缘节点保持通信。各方通过清晰的接口定义与数据协议，共同构成了一个职责分明、协同联动的安全生态体系。

4. 构建验证线下人身安全协同保障体系

4.1. 灾害预警模型

系统动力学[9]基于灾害系统要素的因果反馈关系，构建气象－地质－响应的动态模型。该模型由数据采集层、风险评估层和响应决策层三个核心子系统构成。数据采集层通过实时接入气象局 API，获取降雨量、风速；地质局 API 获取土壤饱和度、岩层位移及用户定位数据，实现多源数据的同步采集与整合。风险评估层采用非线性耦合方程计算实时风险指数，该方程聚焦于从多源数据中筛选出的对灾害风险具有直接及显著驱动力的两个核心动态变量：*rainfall* (降雨量，单位：mm/h)与 $soil_{saturation}$ (土壤饱和度，单位：%)。风速、岩层位移等其余监测数据则作为模型背景参数或用于阈值校准。其数学表达式为：

$$R_t = \alpha \cdot 0.32 \cdot rainfall^{1.7} + \beta \cdot \mathrm{e}^{-\frac{t}{24}} \cdot soil_{saturation} - \gamma R_{t-1}. \tag{19}$$

其中，参数 $\alpha = 0.78$、$\beta = 0.65$、$\gamma = 0.23$ 经由马尔可夫链蒙特卡洛方法拟合历史灾害数据确定[2]，以保障模型参数的统计合理性；响应决策层构建五级应急协议，设定风险阈值 $R_t > 85$，当实时计算的风险指数满足该阈值时，系统自动触发红色预警机制，实现灾害风险的动态响应与决策联动。

4.2. 多维度协同治理机制

为推进跨域灾害治理的协同性，构建数据－技术－管理融合框架，实现路径如图 7 所示。该框架通过数据层、技术层与管理层的深度耦合，达成从风险识别到应急响应的闭环。

数据层由多源异构数据融合，打通气象局、地质局及公安系统等多源通道。针对旅游场景下气象、地质与用户行为的异构特征，构建联邦学习网关[8]。运用 FedAvg 算法聚合跨域梯度以优化模型性能，其梯度更新公式为：

$$w_{t+1} \leftarrow \sum_{k+1}^{K} \frac{n_k}{n} w_{t-1}^{(k)} + N\left(0, 0.5^2\right). \tag{20}$$

其中，$N\left(0, 0.5^2\right)$ 为依据隐私预算 $\varepsilon = 0.5$ 注入的高斯噪声[10]，通过引入噪声扰动，确保在参数聚合过程中实现数据可用不可见，理论上可将协作误差控制在 3.2%以内。

技术层通过安全建模与精准管控，整合智能合约、风险预测 AI 及差分隐私保护模块。基于联邦学习构建的联合模型，能够有效识别跨域风险关联特征。同时，引入动态地理围栏技术，通过时空动态边界定义，实现对风险区域的精准管控，协同提升治理技术效能。

管理层由跨域协同响应闭环连接虚拟防护、跨平台规则引擎与安全中枢。依托风险预测 AI 输出的决策建议，应急 SOP 可自动触发跨平台调用共享接口，指令下发至用户终端，形成识别－响应－反馈的完

整闭环。

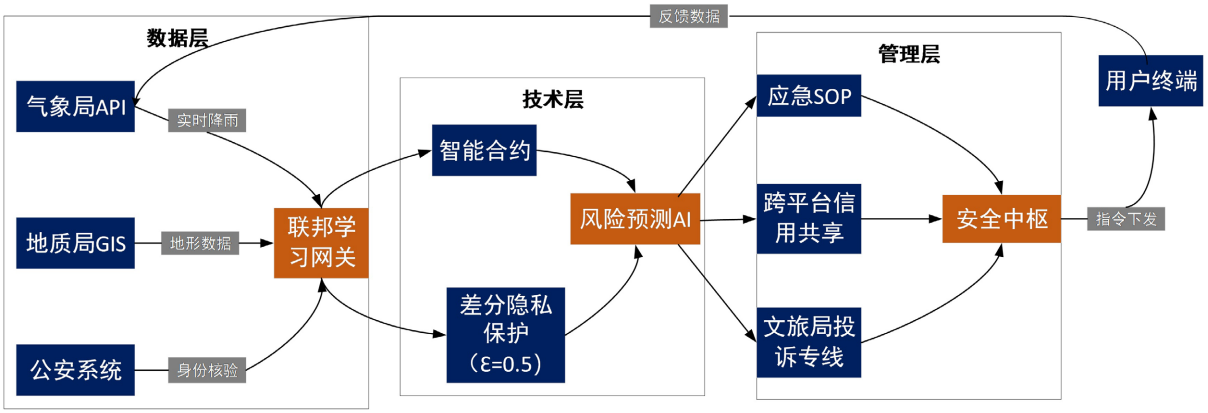

Figure 7. Technical implementation path of cross-domain collaborative governance
图 7. 跨域协同治理的技术实现路径

5. 结论与建议

旅游安全事关人民群众美好生活。本文从满足用户旅游结伴出行安全需求出发，提出建立线上隐私、线下人身及灾害响应多维保障模式，并利用层次分析法计算出 3 大类 26 项核心风险，用联邦学习实现数据可用不可见，借助系统动力学模型提升灾害响应效率，为行业治理提供了有益方案。

为进一步优化安全保障机制，我们将从法律合规与操作落地两个层面推进：首先结合《个人信息保护法》《数据安全法》等法规，明确数据跨域流转的合法边界，确保数据跨境传输符合监管要求；建立数据自动销毁机制，通过智能合约实现数据使用权限的到期自动终止，避免数据超期留存风险；规范智能合约的执行流程，确保合约代码与法律条款的一致性，防止因代码漏洞导致的合规风险。其次，为平台运营者提供标准化的隐私策略配置模板，涵盖数据收集范围、使用目的、存储期限等核心要素，提升用户知情权与选择权的透明度；制定应急响应标准操作程序示例，明确灾害预警触发条件、信息通报流程、救援资源调度等关键环节，确保突发事件下的快速响应与协同处置。

未来需持续推进技术、制度、文化并行建设，让旅游安全治理从被动响应转向主动防控，为行业治理提供有益方案。

基金项目

教育评价改革研究基地(四川省)2025 年度专项课题(2025JPG-C-006)；2025 年四川省大学生创新创业训练计划资助项目(S202510649240X)。

参考文献

[1] 王慧. 社交平台中的搭子社交现象研究——以小红书平台为例[J]. 新媒体研究, 2025, 11(5): 67-70.

[2] 黄佳杰, 巴兆祥. 山地旅游安全事故致因研究——基于“三山五岳”的文本案例[J]. 干旱区资源与环境, 2024, 38(3): 201-208.

[3] 李畅. 手机 APP 用户个人信息保护研究[D]: [硕士学位论文]. 济南: 山东政法学院, 2025.

[4] 网安联. 数说安满周报告[R]. 2024.

[5] 曲忠芳. 35 款 App 违法违规收集使用个人信息 AI 成“重灾区” [N]. 中国经营报, 2025-05-26(C04).

[6] 吴佳佳, 殷杰. 全域旅游安全事故的致因因素与形成路径研究[J]. 安全, 2025, 46(2): 43-49.

[7] 宋才发. 个人信息的保护原则、合理使用与法律保护[J]. 经济与社会发展, 2025, 23(5): 1-10.

[8] 肖雄, 唐卓, 肖斌, 李肯立. 联邦学习的隐私保护与安全防御研究综述[J]. 计算机学报, 2023, 46(5): 1019-1044.

[9] 付丽荣. 大学生旅游安全风险感知的影响因素研究[D]: [硕士学位论文]. 昆明: 云南大学, 2020.

[10] Kairouz, P. and McMahan, H.B. (2021) Advances and Open Problems in Federated Learning. *Foundations and Trends in Machine Learning*, **14**, 1-210. https://doi.org/10.1561/2200000083