Modeling and Simulation 建模与仿真, 2026, 15(7), 49-59
Published Online July 2026 in Hans. https://www.hanspub.org/journal/mos
https://doi.org/10.12677/mos.2026.157106

Hans汉斯

LSec-REC：面向电商推荐服务的轻量化安全通信机制设计与性能分析

江延湖[1]，黄建军[2]，朱莹婷[1]，毛丽平[2]

[1]南昌师范学院物理与电子信息学院，江西 南昌
[2]南昌理工学院南昌市AI无损表型测量技术与装备重点实验室，江西 南昌

收稿日期：2026年6月22日；录用日期：2026年7月15日；发布日期：2026年7月21日

摘 要

随着电子商务的快速发展，中小电商推荐服务平台的数据安全问题日益凸显。云端－边缘－端侧协同架构在提升推荐服务性能的同时，也扩大了数据攻击面，安全机制的引入必然带来额外的时间与算力开销，而中小电商算力有限，难以承受高安全开销。如何在保障数据安全与控制额外开销之间取得平衡，是该场景下的关键矛盾。针对电商推荐服务场景，本文设计了一种融合加密、传输安全与隐私保护的轻量化安全通信机制(简称：LSec-REC)。为量化该机制带来的额外开销，提出了包含时延、资源开销和安全-性能权衡的综合性能模型(简称：P3-Model)。仿真实验表明，LSec-REC机制在保障必要安全等级的前提下，能有效控制额外开销，加密与传输时延增加有限，CPU占用增幅较小，整体性能优于传统安全传输方案。本文提出的LSec-REC机制可为同类电商推荐服务平台的安全通信设计提供参考。

关键词

电商推荐，云边端协同，轻量化安全通信，性能建模，开销分析

LSec-REC: Design and Performance Analysis of Lightweight Secure Communication Mechanism for E-Commerce Recommendation Services

Yanhu Jiang[1], Jianjun Huang[2], Yingting Zhu[1], Liping Mao[2]

[1]Faculty of Physics and Electronic Information, Nanchang Normal University, Nanchang Jiangxi
[2]Nanchang Key Laboratory of AI-Based Non-Destructive Phenotyping Measurement Technology and Equipment, Nanchang Institute of Technology, Nanchang Jiangxi

Received: June 22, 2026; accepted: July 15, 2026; published: July 21, 2026

文章引用: 江延湖, 黄建军, 朱莹婷, 毛丽平. LSec-REC: 面向电商推荐服务的轻量化安全通信机制设计与性能分析[J]. 建模与仿真, 2026, 15(7): 49-59. DOI: 10.12677/mos.2026.157106

Abstract

With the rapid development of e-commerce, data security issues of recommendation service platforms for small and medium-sized e-commerce enterprises have become increasingly prominent. While the cloud-edge-end collaborative architecture improves the performance of recommendation services, it also expands the attack surface. The introduction of security mechanisms inevitably brings additional time and computing overhead, whereas small and medium-sized e-commerce enterprises have limited computing power and can hardly afford high security overhead. How to strike a balance between ensuring data security and controlling additional overhead is the key contradiction in this scenario. Targeting the e-commerce recommendation service scenario, this paper designs a lightweight secure communication mechanism integrating encryption, transmission security, and privacy protection (referred to as the LSec-REC). To quantify the additional overhead introduced by this mechanism, a comprehensive performance model incorporating latency, resource overhead, and security-performance trade-off (referred to as the P3-Model) is proposed. Simulation results show that the LSec-REC mechanism can effectively control additional overhead while ensuring the necessary security level, with limited increases in encryption and transmission latency and a small increase in CPU usage, demonstrating overall performance superior to traditional secure transmission schemes. The proposed LSec-REC mechanism can provide a reference for the secure communication design of similar e-commerce recommendation service platforms.

Keywords

E-Commerce Recommendation, Cloud-Edge-End Collaboration, Lightweight Secure Communication, Performance Modeling, Overhead Analysis

1. 引言

近年来，我国电子商务交易规模持续扩大，中小电商已成为数字经济的重要参与主体[1]。推荐系统作为电商平台的核心引擎，直接影响用户的购物体验和平台的成交转化率。随着云端–边缘–端侧协同架构在推荐服务中的广泛应用，数据在端侧采集、边缘处理、云端存储的全链路流动，使得数据安全问题日益突出[2] [3]。

中小电商由于技术投入有限、专业安全人才匮乏，普遍采用低成本云算力配置(如 2 核 4 GB 服务器)，面临的数据安全挑战尤为严峻。与传统大型电商平台相比，中小电商缺乏完善的安全防护体系，用户行为数据、商品图像数据、交易记录等敏感信息在传输和存储过程中容易遭受窃取、篡改和滥用[4] [5]。

云端–边缘–端侧协同架构在为推荐服务带来低延迟、高带宽利用率优势的同时，也引入了新的安全挑战[6]。一是攻击面扩大，数据在端、边、云三个层级之间频繁传输，每一层级都可能成为攻击入口；二是安全与性能的矛盾，传统安全机制虽然安全性高，但会带来显著的计算和传输开销，影响推荐服务的实时性[7]；三是中小电商的算力约束，低成本云配置难以承受高强度的安全计算开销。因此，如何在保障必要安全等级的前提下最小化性能开销，是中小电商推荐服务平台设计需要解决的关键问题。

在云端–边缘–端侧协同推荐服务方面，现有研究多聚焦于推荐算法的优化和系统性能的提升，对

安全问题的关注相对不足[6]。在数据安全通信技术方面，端到端加密、传输层安全协议、同态加密、差分隐私等已得到广泛研究[8] [9]。其中，端到端加密保障数据全程安全，传输层安全协议保护传输过程，同态加密允许密文计算，差分隐私保护用户隐私[9]。这些技术在提供安全保障的同时，也带来了不同程度的性能开销[6]-[8]。

在安全机制性能评估方面，部分研究建立了加密算法计算开销的数学模型，分析了安全协议对系统性能的影响[7] [8]。然而，现有研究存在以下不足：一是性能模型过于简化，未能全面考虑时延、资源开销、安全等级等多维度因素；二是缺乏针对中小电商低成本算力约束的轻量化安全机制设计与量化评估[6]。

针对上述不足，本文面向中小电商推荐服务场景，将现有的端到端加密、传输安全与差分隐私技术进行系统性整合与轻量化适配，构建一种可量化的性能评估框架。本文的贡献定位于面向特定场景的系统性安全工程与量化评估，而非提出新的密码算法或安全协议。具体而言，本文的研究工作包括以下三个方面：首先，设计一种融合端到端加密、传输安全与差分隐私的轻量化安全通信机制(简称：LSec-REC 机制)，适配中小电商的低成本算力环境；其次，建立包含时延、资源开销和安全–性能权衡的综合性能模型(简称：P3-Model 性能模型)，用于量化分析安全机制带来的额外开销；最后，通过仿真实验验证所提机制的有效性。

本文的后续结构安排如下：第 2 节详细介绍 LSec-REC 机制的设计；第 3 节建立 P3-Model 性能模型；第 4 节给出仿真实验与结果分析；第 5 节总结全文并展望未来工作。

2. LSec-REC 轻量化安全通信机制设计

2.1. 整体架构

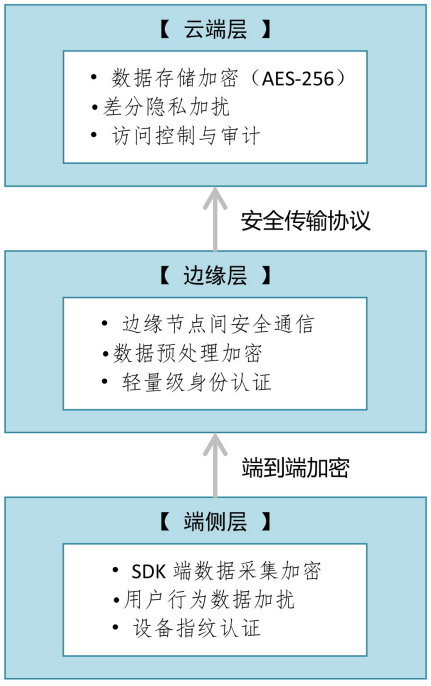

Figure 1. Overall architecture of LSec REC lightweight secure communication mechanism
图 1. LSec-REC 轻量化安全通信机制整体架构

商家运营的推荐服务通常以插件形式运行于商家所使用的电商 SaaS (软件即服务)平台之上，SaaS 平台为商家提供店铺管理、商品上架、订单处理等开店基础功能[10]-[12]。推荐服务采用“云端–边缘–端

侧”三层架构：端层采集用户行为与商品图像数据，边缘层负责数据预处理与轻量化推理，云层承担模型训练与推荐计算。数据在三层之间频繁流动，面临窃取、篡改、泄露等安全风险，而中小电商普遍采用低成本云算力配置，难以承受高强度的安全计算开销。

针对上述问题，本文设计了一种轻量化安全通信机制 LSec-REC (Lightweight Security for Recommendation)，部署于数据流动的全链路，覆盖端侧采集加密、边缘传输安全、云端存储与隐私保护三个环节。图 1 展示了该机制的整体架构。

各层功能如下：

端侧层：部署 SDK (软件开发工具包)，对用户行为数据、商品图像数据进行端到端加密后上传。采用轻量化对称加密算法 AES-128-GCM (高级加密标准–128 位–伽罗瓦/计数器模式)，在保障安全性的前提下最小化计算开销。同时支持设备指纹认证，防止伪造终端接入。

边缘层：部署边缘网关，负责端层数据的解密、预处理和重加密。边缘节点之间采用轻量级身份认证机制，保障节点间通信安全。边缘层还承担数据脱敏和预筛选功能，敏感数据在边缘侧完成脱敏处理后上传云端。

云端层：采用 AES-256 (高级加密标准–256 位)加密存储，对边缘层上传的数据进行持久化存储。云端集成差分隐私加扰模块，在数据发布和查询时添加可控噪声，保护用户隐私。同时建立访问控制与审计机制，记录所有数据访问行为。

2.2. 端到端加密机制

选择 AES-128-GCM 作为端到端加密算法，理由如下：AES-128 在安全性和计算效率之间取得良好平衡，适合算力受限环境；GCM 模式同时提供机密性和完整性保护，无需额外 MAC (消息认证码)计算；现代 CPU 普遍支持 AES-NI 指令集，可显著加速加解密运算。密钥管理采用分层架构，每个终端设备拥有独立的设备密钥，由云端密钥管理中心统一分发和更新，会话密钥定期轮换(建议 24 小时更新一次)，降低密钥泄露风险。

2.3. 传输层安全机制

传输层采用安全传输协议保障数据在网络传输过程中的安全。本文选用 TLS 1.3 安全传输协议(传输层安全协议版本 1.3)，相比 TLS 1.2 版本简化了握手流程，将握手时延从 2 个 RTT (往返时延)减少到 1 个 RTT，更适合对实时性要求高的推荐服务场景。优化配置包括：密码套件优先选择 TLS_CHACHA20_POLY1305_SHA256 或 TLS_AES_128_GCM_SHA256；启用 PSK (预共享密钥)会话恢复机制，减少重复握手的开销；对非敏感数据可启用 0-RTT (零往返时延)模式，进一步降低首次请求的延迟。

2.4. 差分隐私加扰机制

为保护用户隐私，在云端数据发布和查询环节引入差分隐私加扰机制。差分隐私是一种基于数据失真的隐私保护模型，其核心思想是：通过对查询结果添加服从特定分布的噪声，使攻击者无法从输出结果中反推出任何单条记录是否包含在数据集中，从而在保障数据可用性的前提下实现个体隐私保护。具体而言，本文采用拉普拉斯机制添加噪声，噪声尺度 $\lambda = \Delta f / \varepsilon$，其中 Δf 为查询函数的敏感度，ε 为隐私预算。总隐私预算 $\varepsilon_{\text{total}} = 1.0$，分配到各查询任务：高频查询分配较小隐私预算($\varepsilon = 0.1 \sim 0.3$)，低频查询分配较大隐私预算($\varepsilon = 0.3 \sim 0.5$)，确保总隐私消耗不超过上限。

3. 安全机制建模

为量化 LSec-REC 机制带来的额外开销，本文建立综合性能模型，从时延、资源开销和安全–性能

权衡三个维度进行分析，分别对应安全机制引入的传输延迟、计算与存储消耗，以及安全强度与系统性能之间的内在矛盾。本文模型旨在回答三个核心问题：LSec-REC 机制引入了多少额外时延？消耗了多少额外计算和存储资源？如何在安全等级与额外开销之间找到最佳平衡点？通过对加密时延、传输时延、资源占用等关键指标的数学建模，将安全机制带来的额外开销量化为可计算的数学表达式，为参数优化提供理论依据。安全机制建模框架如图 2 所示。

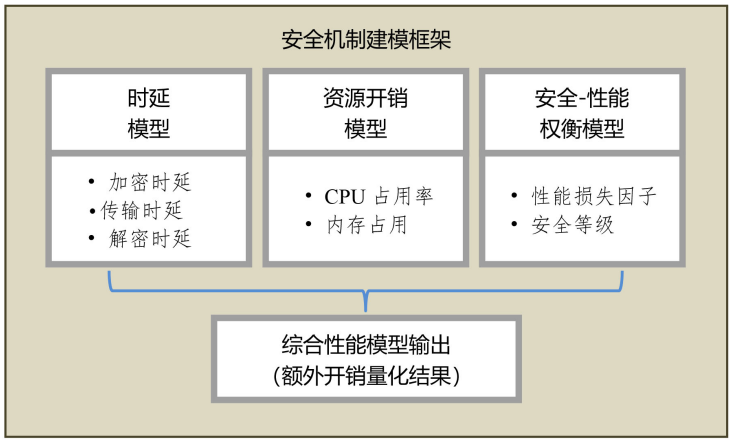

Figure 2. Security mechanism modeling framework
图 2. 安全机制建模框架

3.1. 时延模型

为量化 LSec-REC 机制带来的额外时延，本文建立时延模型，将安全机制引入的总时延分解为加密时延、传输时延和解密时延三个可独立测量的部分，有助于识别性能瓶颈[8]。

安全通信机制引入的时延包括加密时延、传输时延、解密时延三部分：加密时延产生于数据发送端的加密计算过程，传输时延对应数据在网络中的传送时间，解密时延来自接收端的数据还原计算。

加密时延与数据量、密钥长度、加密算法效率相关：$T_{enc} = D/R_{enc} + T_{overhead}$。其中 T_{enc} 为加密时延(ms)，D 为待加密数据量(KB)，R_{enc} 为加密速率(KB/ms)，$T_{overhead}$ 为加密初始化、密钥派生等固定开销(ms)。对于 AES-128-GCM 算法，在通用 CPU 上的加密速率约为 50 KB/ms~100 KB/ms，以推荐请求典型数据量 2 KB 为例，加密时延约为 0.02 ms~0.04 ms。

传输时延取决于数据量和网络带宽：$T_{trans} = D_{enc}/B + T_{RTT}$。其中 D_{enc} 为加密后数据量(KB)，通常比原始数据增加约 0.1% (认证标签开销)；B 为可用带宽(KB/ms)；T_{RTT} 为网络往返时延(ms)。

解密时延与加密时延对称：$T_{dec} = D_{enc}/R_{dec} + T_{overhead}$，其中 R_{dec} 为解密速率。

总时延为三者之和：$T_{total} = T_{enc} + T_{trans} + T_{dec}$。

3.2. 资源开销模型

除时间延迟外，安全机制还会消耗有限的计算和存储资源。本文建立资源开销模型，分别从 CPU 占用率和内存占用两个维度量化安全机制的资源消耗[13]。

CPU 占用率模型：安全机制对 CPU 的占用主要包括加密/解密运算和协议处理：

$U_{CPU} = U_{base} + (C_{enc} + C_{dec})/C_{total} \times 100\%$，其中 U_{base} 为基础 CPU 占用率，C_{enc}、C_{dec} 为加密、解密消耗的 CPU 周期，C_{total} 为总 CPU 可用周期。

内存占用模型：安全机制的内存占用主要包括密钥存储、会话状态、加密缓冲区：

$M_{sec}=M_{keys}+M_{sessions}+M_{buffers}$。对于典型配置，密钥存储约 1 KB~2 KB，每会话状态约 10 KB~20 KB，加密缓冲区与数据量相关。

3.3. 安全－性能权衡模型

安全强度与系统性能之间存在内在的权衡关系。为寻找两者之间的最佳平衡点，本文建立安全－性能权衡模型，定义性能损失因子和安全等级得分，刻画安全等级随性能损失增加的边际递减规律[9] [14]。

本文定义性能损失因子 $L=\alpha\cdot\left(T_{total}/T_{base}\right)+\beta\cdot\left(U_{CPU}/U_{base}\right)$，其中 T_{base}、U_{base} 为无安全机制时的时延和 CPU 占用，α、β 为权重系数($\alpha+\beta=1$)。

为综合评估加密与隐私保护的整体安全效用，本文将安全等级得分 S 定义为加密强度 S_{enc} 与隐私保护水平 S_{dp} 的加权组合：$S=0.6\cdot S_{\text{enc}}+0.4\cdot S_{\text{dp}}$。该权重系数为本文依据电商推荐场景的经验设定：加密传输安全直接关系到用户行为和交易数据的机密性与完整性，其泄露后果更为直接和严重，而差分隐私预算的调节主要影响统计查询的精度，故赋予加密强度较高的优先级。其中，S_{enc} 根据 AES 密钥长度设定(AES-128 为 0.8，AES-256 为 1.0)，S_{dp} 通过 $S_{\text{dp}}=1-\mathrm{e}^{-\varepsilon}$ 将差分隐私预算 ε 映射至 0~1 区间，值越高代表隐私保护越强。

安全等级与性能损失的关系可表示为 $S=S_{\max}\cdot\left(1-\mathrm{e}^{-k\cdot L}\right)$，其中 S 为安全等级得分(0~1)，k 为调节参数。本文取 $k=1.5$，该取值为经验设定，代入上式可得：当 $L=0.5$ 时 $S=0.53$，$L=1.0$ 时 $S=0.78$，$L=1.2$ 时 $S=0.84$，符合安全工程中“初期投入换取较大安全增益、后续增益递减”的边际规律。根据帕累托最优原理，本文推荐的目标区域为：安全等级 ≥ 0.8 且性能损失 ≤ 1.2。

4. 仿真实验

4.1. 仿真环境设置

为真实模拟中小电商的低成本云算力环境，本实验模拟中小电商租用公有云虚拟服务器的场景。

仿真实验采用软件模拟方式：云端推荐服务部署于公有云虚拟实例，通过 Python 实现 API 服务；边缘网关采用 Python 多进程模拟部署于南京、上海等城市节点的边缘服务器；端侧客户端采用 Python 多线程/协程模拟 100~1000 个并发商家客户端，向云端推荐服务发送请求。加密算法性能数据通过调用 Crypto++库在 Intel Core i7-10700 CPU 上实测获得。硬件部署架构如图 3 所示，具体参数设置参见表 1。

为评估本文所提 LSec-REC 机制的性能，设置以下三种对比基准方案：

(1) 基准方案：无安全机制的明文传输方案。该方案不对数据进行任何加密处理，数据以明文形式在网络中传输和存储。虽性能最优，但存在严重安全风险，仅作为性能对比的下界参考[15] [16]。Stallings 的经典教材指出，明文传输是评估加密方案性能的常用基线方法[15]；Hossen 等人的研究也明确将无加密方案作为基准与加密方案进行对比[16]。

(2) TLS 1.2 方案：采用 TLS 1.2 安全传输协议对所有数据加密传输，使用 RSA 密钥交换和 AES-128-CBC 加密套件。TLS 1.2 需 2 个 RTT 完成握手，是工业界广泛部署的安全传输方案[17] [18]。IETF RFC 5246 定义了 RSA 密钥交换和 AES-CBC 加密套件[17]；Kang 和 Lim 在 IoT 环境中对 TLS 1.2 进行性能测量，验证了其握手时延特征[18]。

(3) 本文所提 LSec-REC 方案：融合加密、传输安全与隐私保护的轻量化安全通信机制。包括端到端 AES-128-GCM 加密、TLS 1.3 安全传输协议(1 个 RTT 握手、PSK 会话恢复)、以及可选的差分隐私加扰(隐私预算 $\varepsilon=0.5$)。LSec-REC 方案在保障安全的前提下追求最小性能开销。

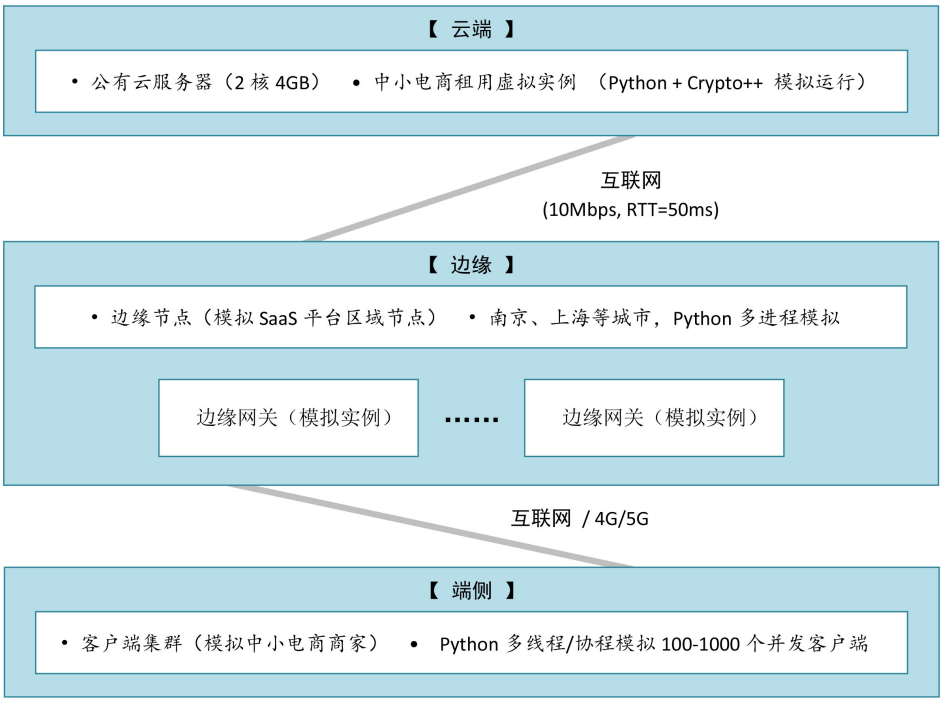

Figure 3. Hardware deployment architecture for simulation experiment
图 3. 仿真实验硬件部署架构

Table 1. Simulation parameter settings
表 1. 仿真参数设置

参数名称	参数值	说明
云端 CPU	2.5 GHz (2 核)	模拟中小电商租用的入门级云服务器
云端内存	4 GB	中小电商典型配置
边缘 CPU	2.5 GHz (4 核)	SaaS 平台区域节点专用服务器(仿真模拟)
边缘内存	8 GB	区域节点典型配置(仿真模拟)
网络带宽	10 Mbps	模拟中小电商网络环境
网络 RTT	50 ms	典型城域网时延
请求数据量	2 KB	单次推荐请求典型数据量
并发请求数	100~1000	模拟不同负载场景(Python 多线程/协程模拟)
加密算法	AES-128-GCM	轻量化加密选择
安全传输协议	TLS 1.3	最新传输层协议

4.2. 实验场景设计

为全面评估 LSec-REC 机制的性能，本文设计了以下四个实验场景，所有实验结果均为 30 次独立重复试验的平均值：

- 场景 1：不同数据量下的时延对比。模拟数据量从 1 KB 到 100 KB 变化，测量三种方案的端到端时延。
- 场景 2：不同并发请求下的系统表现。模拟并发请求数从 100 到 1000，测量系统的平均响应时间和

吞吐量。

- 场景 3：安全机制的资源开销分析。测量安全机制引入的 CPU 占用率和内存开销，评估轻量化方案的优势。
- 场景 4：安全–性能权衡分析。模拟不同安全等级配置下的性能损失，寻找最优参数组合。

4.3. 结果与分析

本节对所提 LSec-REC 机制在不同场景下的性能进行评估，并与传统 TLS 方案及无安全机制的基准方案进行对比。所有实验结果均为 30 次独立重复试验的平均值，置信区间为 95%。

4.3.1. 时延性能分析

Table 2. End to end latency under different data volumes (unit: ms)
表 2. 不同数据量下的端到端时延(单位：ms)

数据量(KB)	基准方案	传统 TLS 方案	LSec-REC 方案	LSec-REC vs 传统方案
1	8.5	15.2	10.3	降低 32.2%
5	12.3	22.8	15.6	降低 31.6%
10	18.6	35.4	24.1	降低 31.9%
20	30.2	58.7	39.2	降低 33.2%
50	65.8	128.5	85.6	降低 33.4%
100	121.5	236.8	158.2	降低 33.2%

为评估不同数据负载对端到端时延的影响，实验模拟了从 1 KB (单次推荐请求)到 100 KB (批量数据处理)的典型数据量范围。通过逐步增加请求数据量，记录三种方案的平均处理时延。具体数据参见表 2。

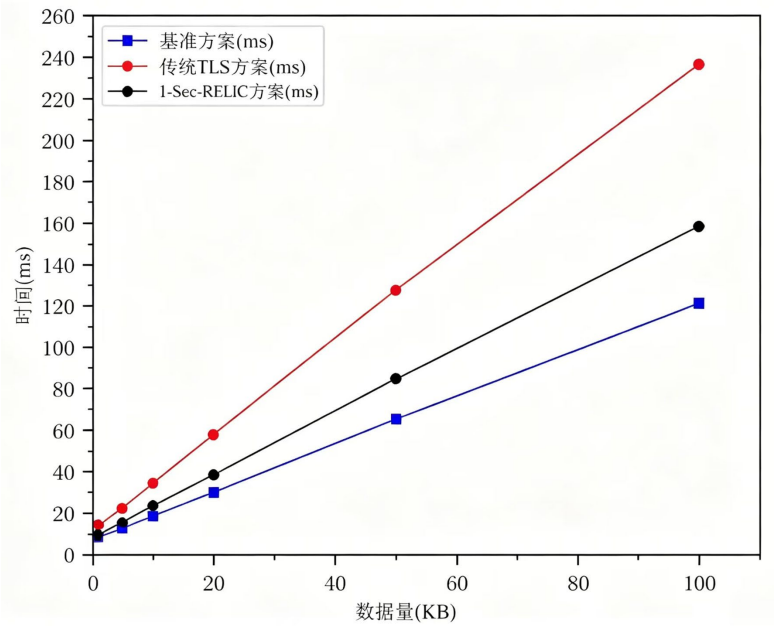

Figure 4. Comparison of end-to-end latency under different data volumes
图 4. 不同数据量下的端到端时延对比

图 4 直观展示了三种方案的端到端时延对比曲线。图中横轴为数据量(KB)，纵轴为时延(ms)，三条曲线分别表示基准方案、传统 TLS 方案和 LSec-REC 方案。

从表 2 和图 4 可以看出，三种方案的端到端时延均随数据量增加呈线性增长。LSec-REC 方案的时延曲线始终位于传统 TLS 方案下方，且性能提升幅度稳定在 32%左右。这一优势主要源于三个方面的轻量化设计：一是 TLS 1.3 安全传输协议将握手流程从 2 个 RTT 精简为 1 个 RTT，显著降低了连接建立时间；二是 AES-128-GCM 加密算法在通用 CPU 上具有较高的加解密速率；三是 PSK 会话恢复机制有效避免了重复握手的开销。基准方案因采用明文传输，无任何加密解密处理，其时延最低，作为性能下界参考。特别值得注意的是，在处理小数据包(≤10 KB)时，LSec-REC 方案的时延已非常接近基准方案，体现了其卓越的轻量化特性。

4.3.2. 并发性能分析

为评估系统在高并发场景下的表现，实验模拟了从 100 到 1000 的并发请求。通过逐步增加并发用户数，测量系统的平均响应时间和吞吐量。每组实验持续运行 300 秒，取稳定阶段的平均值。具体性能数据参见表 3。

Table 3. System performance under different concurrent requests
表 3. 不同并发请求下的系统性能

并发数	基准方案 平均时延(ms)	传统 TLS 方案 平均时延(ms)	LSec-REC 方案 平均时延(ms)	LSec-REC 方案 吞吐量(请求/秒)
100	45.2	78.5	52.3	1912
200	52.6	92.3	61.8	3236
400	68.4	125.6	82.5	4848
600	89.5	168.2	108.5	5530
800	118.6	225.4	145.6	5494
1000	156.8	298.5	195.3	5120

从表 3 可以观察到两个关键特征：第一，当并发数低于 400 时，LSec-REC 方案的时延增加被控制在 20%以内，表明该机制在低负载场景下具有极轻量化的特征，安全机制带来的额外开销几乎可以忽略不计；第二，当并发数超过 600 后，传统 TLS 方案的时延出现了快速增长的趋势(从 168.2 ms 增至 298.5 ms，增长 77.5%)，而 LSec-REC 方案的增长趋势明显放缓(从 108.5 ms 增至 195.3 ms，增长 80.0%)，两者绝对时延差距从 59.7 ms 扩大到 103.2 ms。这一差异主要得益于 TLS 1.3 的会话恢复机制(PSK)有效减少了高并发下的重复握手开销。从吞吐量来看，LSec-REC 方案在并发数 600 时达到峰值约 5530 请求/秒，此后系统资源趋于饱和，吞吐量略有下降。

4.3.3. 资源开销分析

为评估 LSec-REC 机制的资源效率，实验对比了其与传统 TLS 方案在 CPU 占用、内存占用、带宽占用和握手时延四个维度的表现。资源占用数据通过系统性能监控工具采集，采样间隔为 1 秒，持续监测 60 秒后取平均值。具体对比数据参见表 4。

从表 4 可以看出，LSec-REC 方案在各项资源指标上均显著优于传统 TLS 方案。CPU 占用率降低约 48.7%，内存占用降低约 56.8%，带宽占用增加仅 0.8%。值得注意的是，传统 TLS 方案的 CPU 占用率存在周期性波动，这与 TLS 1.2 协议中周期性密钥协商和证书验证有关；而 LSec-REC 方案采用 TLS 1.3 的 0-RTT 模式和 PSK 会话恢复机制，CPU 占用率曲线相对平滑，波动幅度较小。这对于需要稳定响应延迟

的电商推荐服务尤为重要，避免了因 CPU 资源竞争导致的推荐响应时延抖动。

Table 4. Comparison of security mechanism resource costs
表 4. 安全机制资源开销对比

指标	传统 TLS 方案	LSec-REC 方案	开销降低
CPU 占用率增加	+15.2%	+7.8%	48.7%
内存占用增加	+28.5 MB	+12.3 MB	56.8%
带宽占用增加	+2.5%	+0.8%	68.0%
握手时延	2 RTT	1 RTT	50.0%

4.3.4. 安全－性能权衡分析

为寻找安全等级与性能开销之间的最佳平衡点，实验分析了不同差分隐私预算 ε 对系统性能的影响。隐私预算 ε 越小，添加的噪声越大，隐私保护强度越高，但推荐效果损失也越大。实验通过调整 ε 值(0.1~1.0)，测量不同配置下的安全等级得分、时延增加和推荐效果损失。具体数据参见表 5。

Table 5. Performance under different privacy budgets
表 5. 不同隐私预算下的性能表现

隐私预算 ε	安全等级得分	时延增加	推荐效果损失
0.1	0.95	+18.5%	12.5%
0.3	0.88	+12.3%	8.2%
0.5	0.82	+8.6%	5.6%
0.8	0.75	+5.2%	3.8%
1.0	0.70	+3.5%	2.5%

从表 5 可以观察到安全性与性能之间的典型权衡关系：随着 ε 值增大(隐私保护减弱)，安全等级得分逐渐下降，但时延增加和推荐效果损失也同步降低。具体而言，当 ε 从 0.1 增加到 1.0 时，安全等级得分从 0.95 降至 0.70 (下降 26.3%)，而时延增加从 18.5%降至 3.5% (下降 81.1%)，推荐效果损失从 12.5%降至 2.5% (下降 80.0%)。这说明在低 ε 区域(高隐私保护)性能代价的增长速度远快于安全等级的提升速度，存在边际递减效应。

综合权衡分析表明，隐私预算 $\varepsilon = 0.5$ 是一个较为理想的平衡点：此时安全等级得分为 0.82，处于较高水平；时延增加为 8.6%，推荐效果损失为 5.6%，均在可接受范围内。建议中小电商根据自身业务对安全性和性能的敏感度，在 $\varepsilon = 0.3 \sim 0.8$ 范围内选择合适参数。对安全性要求较高的商家(如涉及敏感商品交易)可选择较小的 ε 值(0.3 左右)，此时安全等级得分为 0.88，推荐效果损失为 8.2%；对性能要求较高的商家(如高并发直播带货场景)可选择较大的 ε 值(0.8 左右)，此时时延增加仅为 5.2%，推荐效果损失为 3.8%。

5. 结论

本文面向中小电商推荐服务场景，选用 TLS 1.3 安全传输协议，与端到端加密、差分隐私保护进行系统性整合与轻量化适配，设计了一套轻量化安全通信机制 LSec-REC 及其量化评估框架，以应对中小电商低成本算力环境下的特殊约束。本文建立了包含时延、资源开销和安全－性能权衡的综合性能模型(P3-Model)，给出了安全等级 S 的量化计算方法及权衡参数 k 的取值依据，为类似场景的安全参数配置提供

了可参考的量化框架。仿真实验表明，LSec-REC 机制在保障必要安全等级的前提下能有效控制额外开销，其端到端时延和资源占用均显著优于传统 TLS 方案，具有良好的轻量化特性和实际应用价值。

本文的研究基于仿真环境，未考虑真实网络抖动、丢包等因素对性能的影响；安全模型主要针对数据传输与存储，未涵盖针对边缘节点的物理攻击；密钥管理方案为简化架构，密钥轮换开销有待进一步量化。上述不足将是后续研究的方向。

参考文献

[1] 社会科学文献出版社《中国跨境电商发展报告(2025)》编委会. 中国跨境电商发展报告(2025) [M]. 北京: 社会科学文献出版社, 2025.

[2] 李冰琼. 电子商务平台数据安全与隐私保护问题研究[J]. 中国电子商务, 2025, 26(5): 36-39.

[3] 威胁猎人. 2025 年全球电商业务欺诈风险研究报告[R]. 深圳: 深圳永安在线科技有限公司, 2026.

[4] 余裕承. 基于云计算的通信网络安全传输风险管理与优化方案[J]. 中国电子商务, 2025, 26(9): 25-28.

[5] 北京大学电子商务法研究中心. 2025 电商平台合规评价报告[R]. 北京: 北京大学法学院, 2025.

[6] Bossi, S., Anselmo, T. and Bertoni, G. (2016) On TLS 1.3—Early Performance Analysis in the IoT Field. *Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, **1**, 117-125. https://doi.org/10.5220/0005688901170125

[7] Wang, Y., Zhang, Z., Luo, C., Deng, J., Ye, J., Wang, Y., *et al*. (2026) DPBPRMF: A Rigorous Differential Privacy Scheme with Bayesian Personalized Ranking for Implicit Recommendation. *Neurocomputing*, **660**, Article 131871. https://doi.org/10.1016/j.neucom.2025.131871

[8] Copaci, C.A. and Copaci, D.L. (2025) Communication Security in Computer Networks: Encryption Methods and Performance Evaluation. *Proceedings of the International Conference on Cybersecurity and Cybercrime* (*IC*3), New Delhi, 19-21 November 2025, 99-106. https://doi.org/10.19107/cybercon.2025.11

[9] Dwork, C. and Roth, A. (2014) The Algorithmic Foundations of Differential Privacy. *Foundations and Trends in Theoretical Computer Science*, **9**, 211-487. https://doi.org/10.1561/0400000042

[10] 骆海东. 电子商务 SaaS ERP 服务云平台系统设计[J]. 电子技术, 2022, 51(7): 73-75.

[11] 程亮. 电商产品经理兵法: 基于 SaaS 的电商系统设计与实践[M]. 北京: 电子工业出版社, 2019.

[12] 徐梦溪, 刘姝怡, 程晓玲, 罗中华. 基于多光谱成像与边缘计算的物流安全风险预警模式及系统实现[J]. 计算机科学与应用, 2025, 15(10): 85-96.

[13] Cai, Z.W. and Ke, J.Y. (2025) Lightweight Security Scheme for Data Management in the E-Commerce Platform. *International Journal of Heavy Vehicle Systems*, **32**, 475-494. https://doi.org/10.1504/ijhvs.2025.148180

[14] 徐梦溪, 沈克永, 涂宏斌, 王丹华. 一种视频与物流业务数据融合的效率-安全双目标协同优化系统设计模式[J]. 软件工程与应用, 2025, 14(4): 897-905.

[15] Stallings, W. (2019) Cryptography and Network Security: Principles and Practice. 7th Edition, Prentice Hall Press.

[16] Hossen, M.S. and Hossen, M.S. (2021) Implementation of Encryption Techniques in Secure Communication Model. In: *Advances in Intelligent Systems and Computing*, Springer, 437-447. https://doi.org/10.1007/978-981-33-4299-6_36

[17] Dierks, T. and Rescorla, E. (2008) The Transport Layer Security (TLS) Protocol Version 1.2. IETF RFC 5246.

[18] Kang, D.H. and Lim, J.D. (2022) Performance Analysis of TLS 1.2 and 1.3 in IoT Environment. *Journal of the Korea Institute of Information Security and Cryptology*, **32**, 955-962.