基于智慧服务中台的互联网医院技术架构与安全体系研究

熊炜[1] 张海波[1]温必荣[1]赵霞[1,*]
（[1]南部战区总医院信息科，广州 510510）

[摘要]**目的/意义**针对互联网医院建设中院内业务系统分散、线上线下服务衔接不畅以及患者诊疗数据安全风险等问题，设计面向互联网诊疗场景的智慧服务中台架构与安全保障方案。**方法/过程**以某大型综合医院互联网医院平台为对象，构建以智慧服务中台为核心的技术架构，将患者身份核验、线上诊疗订单处理和关键操作记录统一管理，并通过接口连接院内业务系统、支付平台和监管接口；基于平台试运行期间的业务日志、接口监控记录和审计记录，验证平台在业务衔接、系统运行和操作追溯方面的效果。**结果/结论**应用验证表明，该架构能够支撑互联网医院业务闭环与稳定运行，平台核心服务可用性达到99.93%，订单状态同步成功率达到99.50%，关键业务审计日志完整率达到97.31%。该方案能够支持线上复诊、电子处方、药师审方、支付结算、取药配送和监管记录等业务连续开展，并为互联网医院平台建设提供实践参考。
[关键词] 互联网医院；中台架构；微服务；数据安全

Research on the Technical Architecture and Security System of Internet Hospitals Based on a Smart Service Middle Platform

Xiong Wei[1]Zhang Haibo[1]Wen Birong[1]Zhao Xia[1,*]
([1] Department of Information, General Hospital of Southern Theater Command, Guangzhou 510510, China)

[Abstract] **Purpose/Significance**To address fragmented in-hospital information systems, discontinuities between online and offline services, and risks to the security of patient diagnosis and treatment data in Internet hospital development, this study designs a smart service middle-platform architecture and security assurance scheme for Internet-based medical services.**Method/Process**Using the Internet hospital platform of a large general hospital as the study setting, we developed a technical architecture centered on a smart service middle platform. The architecture centrally manages patient identity verification, online consultation order processing, and key-operation logging, and connects in-hospital information systems, payment platforms, and regulatory interfaces through standardized interfaces. Business logs, interface monitoring records, and audit records collected during trial operation were used to evaluate the platform's performance in business coordination, system operation, and operation traceability.**Result/Conclusion**Application validation showed that the proposed architecture supported closed-loop Internet hospital services and stable platform operation. The availability of core platform services reached 99.93%, the order status synchronization success rate reached 99.50%, and the completeness rate of audit logs for key business operations reached 97.31%. The scheme supported the continuous delivery of online follow-up consultations, electronic prescribing, pharmacist prescription review, payment settlement, medication dispensing or delivery, and regulatory recordkeeping, providing practical reference for the development of Internet hospital platforms.
[Keywords] Internet hospital; middle-platform architecture; microservices; data security

10.12201/bmr.202608.00015V1

1 引言

随着“互联网+医疗健康”政策持续推进以及新一代信息技术在医疗领域的应用深化，互联网医院已成为医院拓展线上医疗服务的重要形式。《互联网诊疗管理办法（试行）》和《互联网医院管理办法（试行）》对互联网诊疗活动、互联网医院准入、诊疗质量、信息安全和监管对接提出了要求。近年来，相关研究从运营管理、服务体系和发展模式等角度总结了互联网医院建设实践，表明其服务内容已由在线咨询、预约挂号等便民服务，逐步延伸至复诊续方、处方流转和诊后管理等环节[1-3]。随着服务环节增多，诊疗流程衔接、患者信息调用与保护以及平台安全运行也成为医院建设中需要同步处理的内容[4]。

围绕互联网医院建设中的系统对接与安全运行需求，已有研究从医疗卫生数字化转型、医疗数据汇聚与安全共享、信息集成平台防护以及线上线下一体化服务安全等方面提出了建设思路[5-7]。同时，服务质量和运营评价研究已将数据安全、诊疗质量和系统运行纳入互联网医院的评价范围[8]。这些研究为平台建设提供了参考，但现有讨论多聚焦于建设原则、安全要求或服务评价。对于诊疗、药学和支付等既有系统如何围绕同一业务流程进行连接并在信息交换过程中保持处理结果一致、关键操作可追溯，仍需结合具体平台建设实践进一步说明。

已有平台实践表明，统一患者标识和接口交换是支持跨系统数据调用的重要基础[9-10]。基于此，本文以某大型综合医院互联网医院平台为对象，构建以智慧服务中台为核心的技术架构。本文建立患者身份、订单编号与关键操作记录之间的关联关系，使线上问诊、电子处方、药师审方和支付结算等环节虽然由不同系统分别处理，但相关结果能够围绕同一患者和同一订单完成更新、核对与追溯；同时，将身份鉴别、权限校验和操作留痕嵌入接口调用过程，使业务处理与安全控制同步进行。最后，本文基于平台试运行期间的业务日志、接口监控记录、订单同步记录和审计记录，对该架构在跨系统业务衔接、稳定运行和关键操作追溯方面的实际效果进行验证。

2 互联网医院建设现存问题分析

2.1 跨系统业务衔接与订单同步问题

互联网医院的线上复诊、电子处方、药师审方和支付结算等业务，需要在诊疗、药学、支付等多个系统之间完成信息调用与结果反馈。现有研究围绕智慧医疗互联、医院信息集成、服务总线和智慧医院技术架构开展了探索，为多系统接入和服务协同提供了参考[11-14]。但在具体建设过程中，同一患者和同一诊疗事项往往在不同系统中对应不同的身份标识、订单编号和处理状态；当接口调用超时、请求重复提交或结果反馈延迟时，容易出现重复录入、订单状态更新滞后和异常订单核对困难等情况。因此，平台需要建立患者身份与诊疗订单之间的关联关系，并将问诊、处方、审方、支付和配送等环节的处理结果及时更新至相关系统。

2.2 访问控制与关键操作追溯问题

互联网医院涉及患者、医生、药师、管理人员及外部服务平台等多类主体，不同主体的数据访问范围和业务操作权限存在差异。医院信息集成平台安全、数据安全治理、线上线下一体化医疗服务安全和医院网络安全等研究表明，身份认证、权限控制、接口防护和日志审计是保障医疗信息系统安全运行的重要内容[15-16]。在病历调阅、处方开具、审方处理、支付退费和监管上报等跨系统操作中，身份校验、权限判断和操作记录若缺少统一关联，订单异常、权限争议和监管核查的处置效率将受到影响。平台需要在接口调用过程中同步完成身份鉴别、权限校验和关键操作记录，并使审计信息能够关联患者、订单、操作人员和处理结果。

3 基于智慧服务中台的互联网医院技术架构

本文提出的互联网医院技术架构以服务渠道、统一服务入口、智慧服务中台和院内基础系统为主体，运营监控与安全保障贯穿各层，如图 1 所示。患者、医生、药师和管理人员通过不同入口访问平台；平台统一完成身份核验、订单处理、消息发送、数据交换和操作记录，并通过受控接口调用院内基础系统。

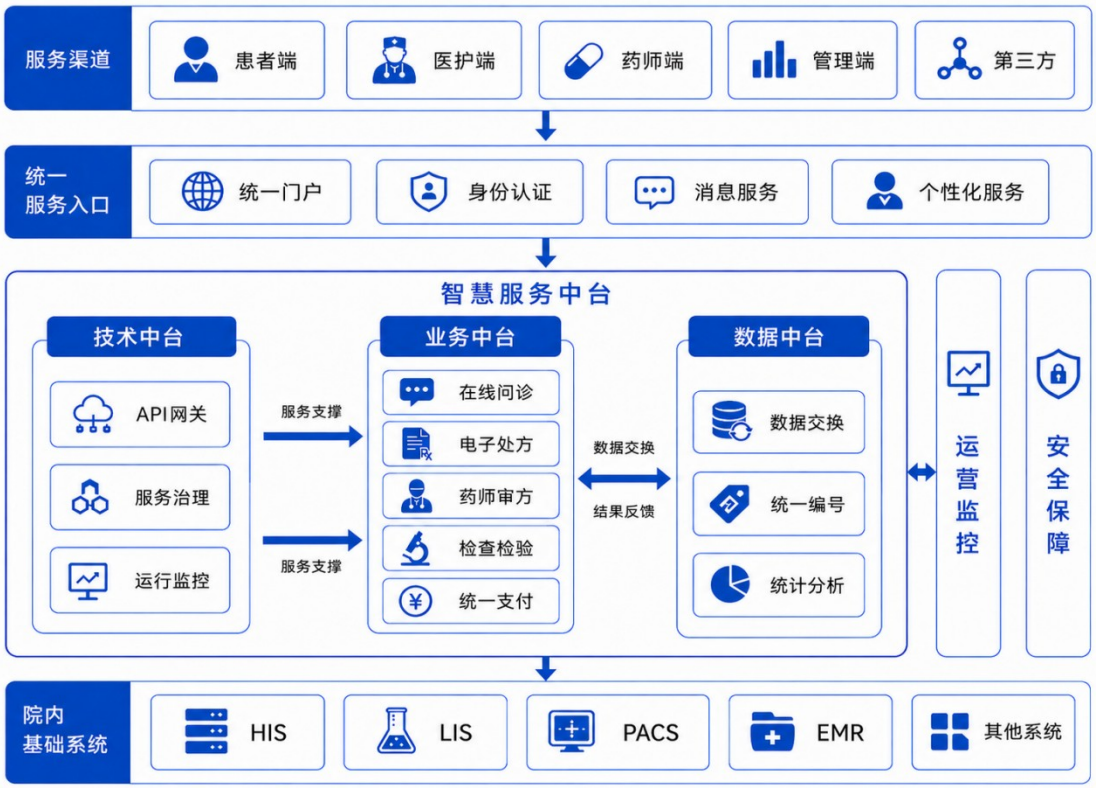

图 1 基于智慧服务中台的互联网医院技术架构

3.1 架构设计

3.1.1 基础设施层

基础设施层为互联网医院提供网络、计算、存储和基础业务数据支撑，并接入医院现有核心业务系统，包括医院信息系统（Hospital Information System，HIS）、实验室信息系统（Laboratory Information System，LIS）、医学影像存档与通信系统（Picture Archiving and Communication System，PACS）以及电子病历系统（Electronic Medical Record，EMR）等。该层采用混合云部署模式：私有云承载敏感医疗数据和核心业务系统，公有云承载预约、消息通知、报告查询等面向患者的非敏感服务，以兼顾医疗数据安全和互联网服务的弹性需求。HIS、LIS、PACS 和 EMR 等系统涉及患者身份、病历、检查检验和影像等信息，部署于院内私有环境；互联网服务区负责统一接入外部访问请求，并向上层应用提供资源调度支持。

基础设施层引入分布式存储与高速缓存系统，支持大规模医疗影像和实时数据流处理。数据吞吐能力 T 可表示为：

$$T=\sum_{i=1}^{m} B_i \cdot \theta_i \quad (1)$$

其中 B_i 为第 i 个存储节点带宽，θ_i 为节点数据处理效率，m 为存储节点总数。以试运行环境中的 3 个存储节点为例，节点有效带宽分别按 280 MB/s、260 MB/s 和 260 MB/s 计算，数据处理效率分别取 0.82、0.80 和 0.80，系统有效吞吐能力约为 645.6 MB/s。该指标可用于评估存储集群在业务高峰期的数据处理余量。

平台采用 Docker 和 Kubernetes 进行容器化部署，实现服务隔离、版本发布、健康检查、弹性伸缩和故障迁移。结合 DevOps/GitOps 流程，对配置变更、版本发布和服务回滚进行统一管理，减少人工部署带来的运行风险。基础设施层同时为 CA 数字证书、身份认证、数据加密和审计追踪等安全措施提供运行支撑，相关安全设计见第 4 章。

3.1.2 智慧服务中台层

智慧服务中台层是医院患者服务体系的基础性支撑平台，为多渠道、线上线下一体化、互联网+医疗服务提供统一的技术规范、用户服务能力与核心运营能力。该平台作为医院患者服务系统的基础底座，由技术中台、业务中台和数据中台构成。

(1) 技术中台

技术中台包括接口网关、身份认证、服务注册、调用监控和日志采集等组件。外部请求进入平台后，首先由接口网关完成访问校验和路由转发，再调用相应业务服务；平台同步记录接口调用时间、调用结果和异常信息，便于后续排查问题。中台采用微服务架构，将传统单体系统拆分为独立运行的细粒度服务单元，每个服务具有独立的生命周期管理与部署能力，从而实现系统弹性与快速迭代。微服务的调用可表示为：

$$R_{total}=\sum_{i=1}^{n}\alpha_i\cdot R_i \quad (2)$$

其中，R_i 表示第 i 个微服务的响应时间，α_i 为服务权重系数。该公式可用于计算整体请求的期望响应时间，以指导弹性伸缩策略。以线上复诊续方流程为例，其关键链路包括身份核验、病历调阅、处方提交、药师审方、支付结算和消息通知等微服务。根据试运行期间接口监控日志，选取各环节平均响应时间分别为 80 ms、210 ms、160 ms、300 ms、180 ms 和 90 ms，并结合链路调用权重 0.10、0.20、0.20、0.20、0.20 和 0.10 进行加权计算。

技术中台还引入服务网格（Service Mesh）与轻量化容器编排（Kubernetes）机制，实现跨系统的统一通信、安全策略、流量治理与熔断控制。Service Mesh 主要用于处理微服务之间的通信治理问题，将服务发现、负载均衡、熔断限流和调用追踪等能力从业务代码中解耦出来，降低业务服务改造成本。Kubernetes 主要用于容器编排和运行状态管理，可结合健康检查、自动重启和弹性伸缩机制提升平台稳定性。通过统一接口规范和参数化接口设计，使外部系统可以灵活接入，实现院内外系统的互操作性。

(2) 业务中台

业务中台依托微服务框架、API 网关、服务注册与发现及工作流引擎，将线上问诊、电子处方、药师审方、支付结算和药品配送等业务拆分为可独立调用的服务单元。平台通过工作流规则确定服务调用顺序，并借助消息机制传递审方、支付和配送等处理结果。例如，处方审方通过后，系统将审方结果发送至支付、配送和监管相关服务，各服务完成处理后返回结果并更新订单状态。该设计减少了业务系统之间的直接耦合，并为接口超时、重复提交和状态异常等情况提供了处理依据。

(3) 数据中台

数据中台以数据集成、数据治理和数据服务为基础，通过患者主索引和统一数据模型关联院内临床系统与支付、消息等外部服务的数据。平台对患者、就诊、订单、处方、检查检验和支付等信息进行字段映射与编号关联，使各业务服务能够按需获取数据，并将处理结果同步至相关系统。数据仓库和实时处理组件进一步汇总业务运行、订单流转和接口调用数据，用于异常订单核对、运行监测和运营统计。

技术中台负责接口接入、身份认证和运行监控，业务中台负责诊疗流程处理与订单状态更新，数据中台负责数据关联和交换，三者共同连接患者端、医务端、药师端、管理端以及院内外相关系统。

3.1.3 服务应用层

服务应用层面向患者、医护人员、药师和管理人员提供相应业务入口。患者端提供预约挂号、线上复诊、报告查询、支付和配送查询等服务；医护端支持 CA 数字证书登录、病历调阅、在线问诊和电子处方开具；药师端用于处方审核及相关配送信息处理；管理端用于查看业务量、订单处理情况、接口运行状态和监管记录。各类用户通过统一身份和订单信息访问相关服务，线上问诊、处方审核和支付结算等环节完成后，处理结果同步更新至对应系统。管理端汇总业务运行和审计数据，为日常运维、质量管理和监管核查提供依据。

3.2 线上复诊续方流程设计

图 2 展示了平台支持的线上复诊续方流程。在该场景中，患者通过统一入口完成实名核验后，平台关联既往就诊记录，并向医生端提供病历、检查检验结果和历史用药信息。医生完成在线问诊并开具电子处方后，处方进入药师审方环节；审方通过后，平台生成支付订单，并将支付结果同步至处方、药房或配送等相关系统。各环节围绕同一患者和订单编号更新处理状态，接口调用时同步完成身份校验、权限判断和操作记录。当出现接口超时、重复提交或结果返回延迟时，工作人员可依据患者编号、订单编号和操作日志进行核对与处理。

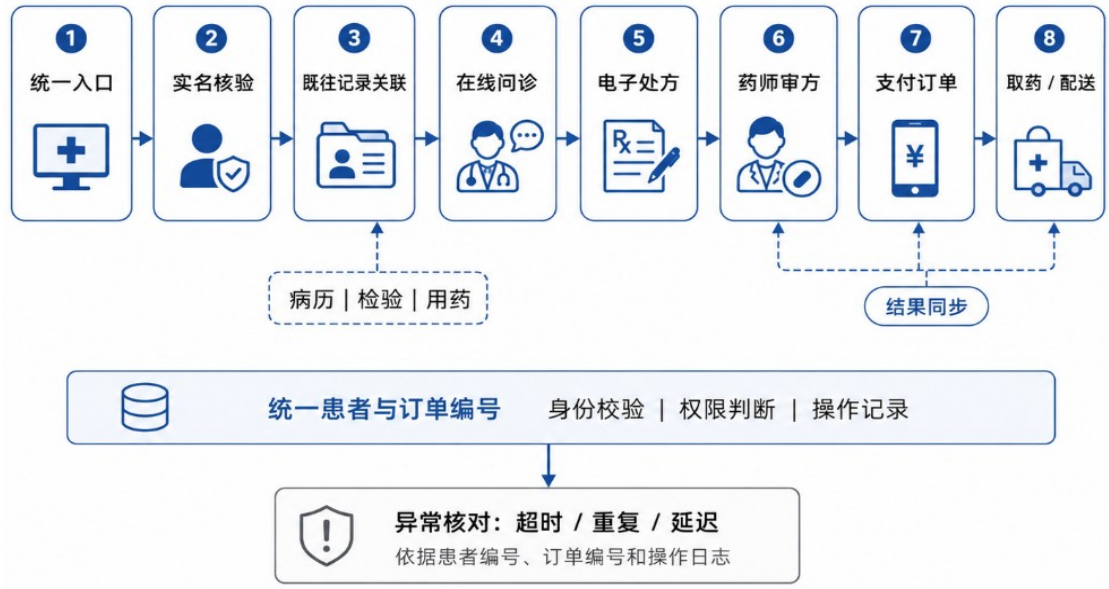

图 2 线上复诊续方流程

4 安全保障体系设计

依据 GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》[17]等要求，并结合互联网医院线上复诊、电子处方、药师审方、支付结算和监管上报等业务场景，本文构建覆盖身份认证、权限控制、接口防护、数据保护、操作审计和运行保障的安全保障体系。平台由统一接入网关、认证中心、权限服务、业务服务、审计服务和安全监测组件构成。外部请求进入平台后，依次完成传输加密、身份验证和接口鉴权；业务服务处理处方审方、支付、退费和监管上报等操作时，根据用户角色和数据范围进行权限校验，并记录关键处理过程。具体控制措施如表 1 所示。

表 1 安全保障体系

安全层级	实施方式	关键技术措施
终端安全	终端请求携带用户令牌、设备标识和来源信息，经网关校验后进入业务服务	实名核验、设备指纹、短时令牌、异常登录识别
应用安全	网关统一鉴权，业务服务调用权限服务校验角色、资源和数据范围	接口网关、接口限流、幂等校验、关键操作审计
系统安全	服务运行于容器集群，发布前完成镜像扫描，生产运维统一接入	镜像扫描、安全基线、堡垒机、补丁管理、字段级加密
网络安全	互联网接入区、应用服务区和核心数据区分域部署，跨域访问通过受控接口完成	防火墙、服务网格、双向传输层安全协议（Transport Layer Security，TLS）
物理安全	核心节点冗余部署，关键数据和审计日志定期备份	门禁监控、温湿度监测、数据备份、异地容灾

4.1 身份认证与权限控制

平台通过认证中心、访问令牌和权限服务完成用户身份确认与访问控制。患者通过实名核验、手机号校验和就医码绑定完成身份确认；医生、药师和管理人员通过账号口令、动态验证码或 CA 数字证书登录。认证通过后，认证中心生成短时访问令牌，并记录用户编号、角色类型、机构信息、设备标识和会话有效期。用户再次访问业务接口时，接口网关校验令牌有效性、设备信息和访问来源。

权限控制结合用户角色、岗位职责、接诊关系和数据范围进行判断。医生在当前接诊范围内调阅病历和开具处方；药师仅访问审方所需的处方、用药信息及相关病史；管理人员根据岗位权限查看运营、质控和监管数据。病历调阅、电子处方、药师审方、支付结算退费和数据导出等关键操作均需经过权限服务校验。

4.2 接口防护、数据保护与审计留痕

外部请求统一经接口网关进入平台，由网关完成接口签名校验、访问频率控制、异常参数拦截和限流熔断。电子处方、支付和退费等接口设置幂等标识，业务服务根据处方号订单号和操作流水号判断请求是否重复，减少重复提交和订单状态异常。处方开具、审方

通过或驳回、支付成功、退费申请和监管上报等关键事件通过消息队列写入审计服务，避免审计记录影响主业务处理。

平台采用传输加密、敏感字段保护和环境隔离等措施保护诊疗数据。病历、处方、支付和身份信息通过 TLS 加密传输；身份证号、手机号、病历摘要、处方内容和支付流水等敏感字段采用加密或脱敏方式保存。业务库与审计库分离部署，审计服务独立保存历史记录；测试环境使用脱敏数据，避免生产环境中的病历、处方和身份信息进入开发测试过程。

4.3 网络隔离与运行保障

平台按照业务敏感程度划分互联网接入区、应用服务区、核心数据区和运维管理区。患者端、医生端和第三方渠道请求首先进入互联网接入区，经防火墙和接口网关过滤后转发至应用服务区；HIS、EMR、LIS 和 PACS 等院内核心系统部署于核心数据区，中台通过受控接口或数据交换服务调用所需数据，不直接开放核心业务数据库访问。系统之间的调用记录接口来源、调用时间、处理结果和异常信息，为故障定位和安全核查提供依据。

在运行保障方面，容器镜像发布前进行漏洞扫描和依赖检查，高危漏洞镜像不得进入生产环境。生产运维通过堡垒机统一接入，数据库变更、配置调整、服务发布和日志导出均保留操作记录。核心服务器、数据库和存储采用冗余部署，电子病历、电子处方、支付记录和审计日志定期备份，并开展恢复验证，以保障关键业务在设备故障或环境异常情况下持续运行。

5 部署与运行验证

本文以某大型综合医院互联网医院平台为对象，基于 2025 年 6 月至 2026 年 4 月试运行期间的脱敏业务日志、接口监控记录和审计记录，验证智慧服务中台架构在业务支撑、系统运行和安全保障方面的适用性。平台面向患者、医生、药师和管理人员提供服务，覆盖线上复诊、预约挂号、报告查询、电子处方、药品配送和运营监管等场景。

5.1 业务运行与流程闭环验证

运行期间，平台在保留院内核心业务系统原有职责的基础上，通过智慧服务中台连接诊疗、药学、支付、消息和监管等系统，实现患者身份关联、订单处理、信息交换和操作记录。平台累计服务约 130.8 万人次，完成线上预约及缴费 115.4 万笔、线上复诊与咨询 4492 单、药品配送 172 单，主要运行情况见表 2。

表 2 平台业务运行与流程闭环验证结果

验证维度	验证内容	结果
服务规模	累计服务人次	130.8 万人次
线上服务	线上预约及缴费、线上复诊与咨询	115.4 万笔、4492 单
配送服务	药品配送订单	172 单
系统接入	院内业务系统、支付平台、消息平台、监管接口	实现统一接入与服务封装
流程追溯	身份核验、病历调阅、处方开具、药师审方、支付配送	关键环节均配置日志记录

以线上复诊续方为例，患者完成身份核验后，医生在线调阅既往记录并开具电子处方，处方经药师审核后进入支付及取药或配送环节。各环节的处理结果和关键操作均按患者与订单编号记录，为业务状态更新、异常订单核对和后续追溯提供依据。

5.2 系统性能与稳定性验证

基于试运行期间的接口调用日志、系统监控数据、订单同步记录和审计日志，对平台运行情况进行统计，结果见表 3。平台核心服务可用性为 99.93%，核心业务接口调用成功率为 99.62%，订单状态同步成功率为 99.50%；主要业务接口平均响应时间和 95%分位响应时间分别为 236 ms 和 721 ms。节点故障模拟及运维切换过程中，平台通过负载均衡和容器编排完成服务迁移，核心服务恢复时间控制在 60 s 以内，未出现单节点故障导致的全局业务中断。

表 3 平台系统性能与稳定性验证结果

验证维度	验证指标	结果
服务可用性	核心服务可用性	99.93%
接口性能	平均响应时间、95%分位响应时间	236 ms、721 ms
调用稳定性	核心业务接口调用成功率	99.62%
业务协同	订单状态同步成功率	99.50%
故障恢复	核心服务恢复时间	≤60 s

验证维度	验证指标	结果
安全运行	审计日志完整率、已确认数据泄露事件、越权访问安全事件	97.31%、0 次、0 次

表 3 结果表明，平台在试运行期间能够保持较稳定的服务可用性、接口调用和订单同步状态。审计日志覆盖身份核验、病历调阅、处方开具、审方、支付和配送等关键操作；在本研究统计期内，未发现经确认的数据泄露事件和因越权访问导致的数据安全事件。上述结果为平台运行监测、异常订单核对和关键操作追溯提供了数据依据。

6 结语

本文以某大型综合医院互联网医院平台为对象，围绕患者身份核验、订单处理、电子处方、药师审方、支付结算、消息通知和操作记录等环节，设计了智慧服务中台架构与安全保障方案。平台通过接口连接院内业务系统、支付平台、消息平台和监管接口，并在业务调用过程中设置身份认证、权限校验、接口防护、数据加密和审计记录。试运行数据表明，平台能够支持线上复诊、处方审核、支付和配送等业务连续处理，并在服务可用性、订单状态同步和审计记录方面保持稳定运行。

未来可围绕跨机构数据交换、监管接口适配和安全事件处置等场景开展进一步验证，以完善互联网医院在数据共享和安全运行方面的技术支撑。随着技术架构和安全体系不断优化，互联网医院有望在保障患者权益、提升医疗服务效率和促进医疗资源协同配置方面发挥更大作用。

作者贡献：熊炜负责研究设计、论文撰写；张海波、温必荣负责文献收集与整理；赵霞负责提供指导、论文修订。

利益声明：所有作者均声明不存在利益冲突。

参考文献

[1] 罗利,付颖,徐雪茹,等.多方参与的互联网医院运营管理研究综述[J].工业工程与管理,2024,29(4):205-222.
[2] 张瑞霖,王禹尧,余俊蓉,等.公立医院互联网医院运营管理的思考与实践[J].中国卫生信息管理杂志,2024,21(1):99-104.
[3] 池慧, 郭珉江, 李亚子, 等. 互联网医院蓝皮书：中国互联网医院发展报告（2024）[M]. 北京: 社会科学文献出版社, 2024.
[4] 姚瑶,崔宇杰,栾伟,等.医疗卫生数字化转型：挑战、策略与未来展望[J].中国卫生经济,2025,44(1):5-10.
[5] 陈大鹏,庄严,张军雁,等.区域健康医疗大数据汇聚、存储、安全共享机制研究[J].解放军医学院学报,2025,46(1):89-95.
[6] 严晓明,陈永辉,潘天祥,等.医院信息集成平台安全体系构建与应用研究[J].中国卫生信息管理杂志,2023,20(5):677-682+688.
[7] 汪兆来.线上线下一体化医疗服务模式下医院网络安全管理研究[J].中国医疗设备,2025,40(6):93-99.
[8] 张晨阳,李培艺,李为民.我国互联网医院服务质量评价指标体系构建[J].医学与社会,2023,36(10):72-78.
[9] 尚诗,陈慧,宓林晖.数字化转型背景下智能出入院服务平台的探索与实现[J].中国医疗设备,2025,40(6):82-86+99.
[10] 曾霞,江俊伸,牟书娟.公立医院互联网医院服务体系的建设和运营探索[J].中国数字医学,2023,18(1):107-111.
[11] 李思宇, 林济南, 张军雁, 卢若谷, 肖志禹, 何昆仑, 庄严. 多级互联智慧医疗系统的研究与建设[J]. 解放军医学院学报, 2025, 46(2): 140-145, 152.
[12] 黄宗浩,王奕,王正源,等.基于医院信息系统的 ESB 高可用架构建设探索与应用[J].中国医疗器械杂志,2022,46(03):342-345.
[13] 马群圣,袁骏毅,岑星星.基于 SOA 的多元化服务总线平台的设计与实践[J].中国医疗设备,2025,40(2):52-58.
[14] 徐安琪,范春.智慧医院技术架构与应用场景体系建设研究[J].医学信息学杂志,2025,46(7):74-79+90.
[15] 郭敬鹏,冯国斌,刘艳亭,等.医院数据安全治理框架设计及实践路径探讨[J].中国卫生信息管理杂志,2022,19(6):879-883.
[16] 王弢,金蕾.医院云计算安全防护中基于 SDN 架构的网络安全平台建设应用[J].医学信息学杂志,2026,47(01):90-93+101.
[17] 国家市场监督管理总局, 国家标准化管理委员会. 信息安全技术 网络安全等级保护基本要求: GB/T 22239—2019[S]. 北京: 中国标准出版社, 2019.