·智慧医疗· doi:10.3969/j.issn.1671-8348.2021.21.029
网络首发 https://kns.cnki.net/kcms/detail/50.1097.r.20210918.0647.004.html(2021-09-22)

智慧医院医疗数据安全交换平台的设计与实现*

段 然,杨聚加#,周来新△
(陆军军医大学第一附属医院,重庆 400038)

[摘要] 智慧医院是当前医院信息化建设的热点,其中数据安全交换平台保障医院内外数据交换需求和不同场景下数据安全交换。以陆军军医大学第一附属医院智慧医院建设为样本,在调查分析基础上自主创新设计基于软件定义网络、软件定义安全的虚拟化组件数据安全交换平台。该文介绍了建设的必要性、建设内容、总体框架、实现目的等,旨在为智慧医院建设提供安全支撑,为智慧医院建设累积经验、提供借鉴。该系统为作者自主创新设计且全国首创的互联安全管理平台体系,改变了现有安全产品结构和布局模式,功能较现有硬件安全产品模式更加全面和完善,全面实现了数据流、控制流的可视化、透明化及智慧监管,代表未来网络信息安全建设发展方向,具有划时代的指导意义。目前已初步实现该安全交换平台建设理念,相应多个软件著作权和发明专利正在申请中。

[关键词] 智慧医院;数据交换;数据安全交换平台
[中图法分类号] R197.323 [文献标识码] A [文章编号] 1671-8348(2021)21-3740-06

Design and implementation of smart hospital medical data security exchange platform*

DUAN Ran, *YANG Jujia*#, *ZHOU Laixin*△
(*First Affiliated Hospital*, *Army Military Medical University*, *Chongqing* 400038, *China*)

[**Abstract**] Smart hospital is a hot spot in the current hospital information construction, in which the data security exchange platform guarantees the data exchange needs inside and outside the hospital and the data security exchange under different scenarios. With the construction of southwest hospital intelligent hospital as the sample, on the basis of investigation and analysis, the virtualization component data security exchange platform is designed by the independent innovation based on the software defined network(SDN), software defined safety(SDS). This paper introduces the construction necessity, construction contents, overall framework and realized purpose to provide the security support for smart hospital construction, accumulate the experience and provide reference for smart hospital construction. This system is the author′s independent innovation design and the country first interconnection security management platform system, which changes the existing security product structure and layout mode, the functions are more comprehensive and perfect compared with the existing hardware security product model, fully realizes the visualization, transparency, and wisdom regulation of the data flow and control flow, represents the development direction of future network information security construction, has the epoch-making guidance significance. At present, the construction concept of the secure exchange platform has been preliminarily realized, and a number of corresponding software copyrights and invention patents are under application.

[**Key words**] smart hospital; data exchange; data security exchange platform

2016 年 10 月中共中央、国务院印发了《“健康中国 2030”规划纲要》,要求各地区各部门结合实际认真贯彻落实[1]。2018 年国务院办公厅出台了《关于促进“互联网+医疗健康”发展的意见》[2],相继全国各地先后出台相关智慧医疗建设规划,全面开启了智慧医院建设。智慧医院建设目标为利用信息化、智慧化等

* 基金项目:重庆市科卫联合医学科研项目面上项目(2019MSXM093);重庆市科卫联合医学科研项目面上项目(KW314)。 作者简介:段然(1977—),高级工程师,在读博士研究生,主要从事智慧医院建设、医疗信息化、人工智能和大数据开发、网络安全等方向的规划和研究。 # 共同第一作者:杨聚加(1986—),工程师,硕士,主要从事医疗信息化、数字孪生、网络安全等方面的研究。 △ 通信作者,E-mail:zhoulaixin@sina.com。

技术手段优化就医流程、增强医疗机构便民服务能力、改善患者就医体验与提升医疗救治水平，切实解决广大人民群众看病难、看病贵及因优质医疗资源不均引起的各种医疗问题，甚至因医疗数据和患者隐私等泄露引起的医患矛盾，具有划时代意义和作用。

当前，智慧医院体系建设是运用云计算、边缘计算、互联网、大数据、区块链、空间计算、人工智能、超融合、物联网、云一网一端融合等新一代信息化技术[3]，与现有业务深度融合或全新设计进而打造全新的智慧型信息化医院，实现从数据到应用、从业务到网络的全面可视化管理，并形成具备数据分析挖掘、AI 建模反射、效益精细化和服务精准化管理的全方位医疗信息体系。该体系建设数据为核心，安全是保障，但往往数据安全容易被忽略，特别是边界的数据交换更是所有医院内部业务与外部其他业务进行数据交互时无法避免的业务链条（医保、预约、银医、互联网医院、集团医院模式、区域协同、远程会诊等），因此，如何实现并确保边界医疗数据安全进行交互成了极具意义且亟须解决的问题。在这种背景下本院自主规划设计了智慧数据安全交换平台，采用全新软件定义网络（software defined network，SDN）/网络功能虚拟化（network functions virtualization，NFV）体系架构，以保障医院内外互联需求和场景下数据安全交换，除取代现有传统的下一代防火墙、安全交换网闸、数据库及行为审计等功能外，还具备统一管理界面、数据流、控制流全面监管、元数据的处理和智能动、静态脱敏、态势感知等安全能力，为互联医疗业务开展提供了一个安全、智慧、便捷高效地运行环境。

1　现状分析

当前，本院业务内网是以医院信息系统为核心，实验室信息系统、影像归档和通信系统为辅助，外挂对外医疗业务为途径的简单传统交换安全模式，其建设思路以网络数据传输为核心，采用传统硬件设备进行区域隔离与控制的方法，配合路由、NAT、ACL 和包过滤等传统安全检测和防御手段，实现与外联业务的互联互通。目前，本院现有对外连接业务主要包括医保、一卡通、银医、预约、支付宝、卫生健康委等，且每条连接均有独立的网络体系支撑对外进行数据交换。交换体系由内、外两部分网络组成，共计 3 台防火墙组成，外部网和内部网仅各部署 1 台前置机，内部访问链路路由至 1 台三层交换机上，通过 ACL 作为最后的控制节点。该体系主机负荷较大，基本没有安全缓冲区，更没有应用层和数据层的管理及监控措施，管理极为不便且各自为政，甚至存在因网络技术员管理不规范、操作流程简化与粗心等客观因素而引发的各种安全风险事件频发。

2　下一代网络安全架构体系

2.1　SDN/NFV 架构

SDN 已被业界内人士和广大网络安全生产厂商认为是一种具有打破传统硬件格局的创新型网络架构，其采用的是以软件定义的方式改变现有硬件防护的模式，主要设计理念为将网络控制与数据转发这 2 个平面从硬件一体化的基础上实现由软件进行分离[4]，将网络应用与网络服务、网元设备之间的相互交互融合紧密地连接在一起，其不在乎也不关注利用何种载体，通过一个逻辑层面上的网络控制集中进行可编程化控制，并协调与网元设备进行交互的应用程序，以及保障应用与网元设备之间的通信与传输[5]。SDN 体系架构可以分为 3 层，即基础设施层、控制层和应用层。基础设施层与控制层之间的交互是通过控制数据平面接口（南向接口）[6]，控制层与应用层之间的交互是通过应用程序编程接口（北向接口），这样通过南北向接口之间的交互[7]，就可构建全局的网络视图，不仅实现了传统网络架构中控制平面的功能，同时实现了各种不同的网络应用，使网络的转发行为能通过软件进行灵活且自主定义和编排，达到网络具备智能化的作用。SDN 架构见图 1。

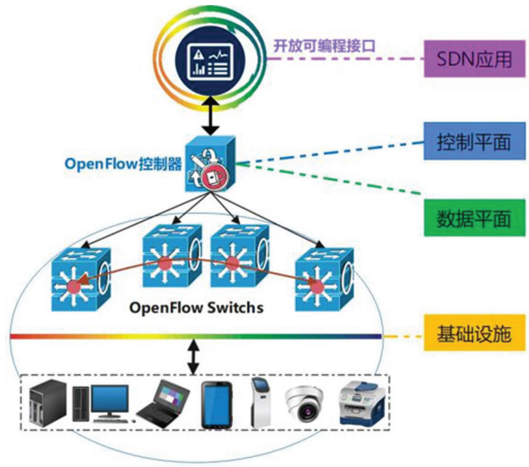

图 1　SDN 架构

NFV 是将基于传统物理硬件的主要网络设备（如服务器、核心交换机、存储单元、GPU、路由器等）采用虚拟化或超融合架构的方式重新构建一个具备自动感知与运维的网络服务基础架构，将这些硬件基础设施提供的功能以软件或虚拟化的形式部署在 VM 上或云平台内，用以承载传统 CT 和 IT 应用，从而实现软与硬件之间的完全解耦合，使这些基础硬件提供的网络与应用功能不再依托于硬件上运行，以达到资源之间可充分复用和共享，同时便利于后期更多的业务能够在此基础上进行快速部署、应用及开发[8]。当然，NFV 的另一个更重要的特点就是通过采用虚拟化方式的部署可以在业务需求突发变化时，其自身可以进行内部自动部署和调整、故障自我隔离和自愈及应用弹性伸缩等[9-12]。NFV 架构可以分为 3 个层次，即 NFV 基础硬件设施层、网络功能虚拟应用层和 NFV 管理与编排层，其架构见图 2。

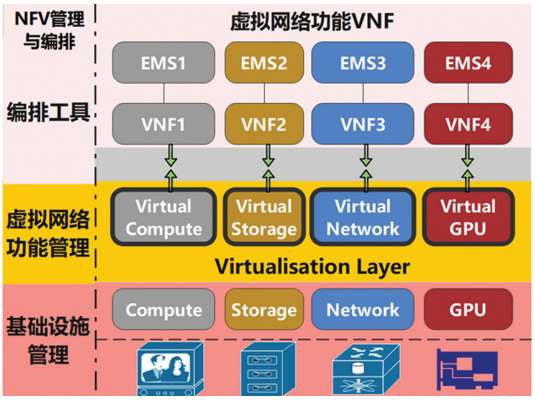

图 2 NFV 架构

NFV 与 SDN 在基础设施层采用的技术是基本上一致的，大都是采用 X86 通用服务器，利用云计算和虚拟化技术这一些技术来实现的，同时二者相互独立，又存在互补关系，因此，二者相融合必将构建一种全新的智慧型网络创新架构，具备无穷的潜在价值。该架构的网络必然是可编程的、健壮的、可开发的、可互操作的、虚拟和物理共存的，且具备与云进行融合的自愈型网络构架。

2.2 软件定义安全(software defined security，SDS)架构

SDS 架构是一种全新的安全架构，与传统安全架构存在明显不同，但从来都不是一种标准，其具备安全自动化、安全信息智能化、移动目标防御及可编程性等功能，不仅能实现安全策略自动配置下发、安全资源自动化调度管理和自主编排安全功能，同时也能抽象底层安全设备，将独立的、存在差异的安全设备抽象成统一的安全资源，形成透明、统一的模式提供给管理者。该架构包括安全应用、安全控制平台和开发安全设备三部分，具有开放的生态环境、控制平面与数据平面分离、可编程的安全能力和与网络环境松耦合等特点，其架构与 SDN 相似，但强调的是通过将安全控制平面上移，因此，结合 SDN/NFV 技术可实现安全网元设备快速部署与应用，且灵活统一管理安全资源。SDS 架构见图 3。

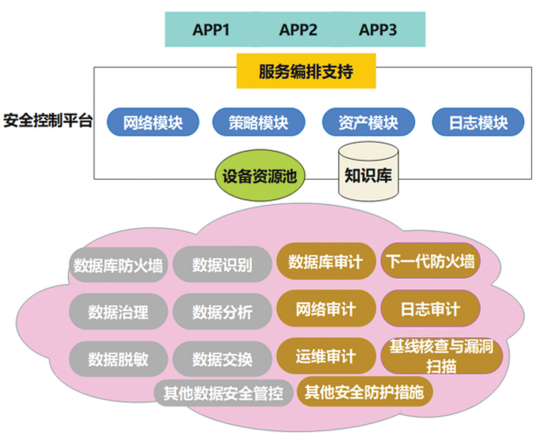

图 3 SDS 架构

3 平台体系设计

本院智慧数据安全交换平台采用并融合了国际上先进的体系架构与设计理念，自主研发并设计将 SDN、NFV 和 SDS 三者进行深度融合，从而构建功能复用、数据共享、防护一体化、数据流向、管理全面可视化的创新网络架构。该架构是采用 Open Stack 等与超融合架构作为平台运行基础环境，根据平台运行要求及业务需求增长可方便、任意的增加底层硬件以获得性能和空间上的提升；平台采取统一界面管理，内部所有功能均是一级界面控制，且所有功能及经过平台的数据都能全面管控和可视化展示；平台功能组件均采用虚拟组件方式部署，取代传统的安全硬件来实现全部安全功能，方便统筹交换和数据流管理，虚拟组件包含但不限于防火墙、入侵防御、行为管理、WEB 防火墙、VPN、审计系统(日志、网络、数据库、运维、行为)、基线核查漏洞扫描、网络态势感知分析、动静态脱敏、数据防泄露等。该平台体系构架首创新颖，安全和管理功能全面且完善，实现从业务、控制数据等全方位管控，功能结构、数据清晰透明，遵循等级保护 2.0 原则，在医疗网络和互联网、专用网间构建了一个全新的边界防护体系，其具有领先、实用和指导的重要意义，将为今后医疗行业甚至国家网络安全与建设提供另一种不同以往的建设思路。

平台建设既要保障基础设施底层安全、业务应用、数据交换等多源异构化的安全防护需求，也要构建智慧型网络安全分析决策中心与统一运维管理中心[11]。通过对多维度安全事件进行针对性的建模，将入侵检测、病毒特征匹配及威胁漏洞等基础性安全防护能力采用规范化、标准化方式进行封装，建立具备可视化、编排性及流程化的调度安全技术和能力体系，以保障针对平台的各类安全事件与威胁、不同安全应用场景的自动化防御和处置。平台体系架构见图 4。数据安全交换平台网络拓扑见图 5。

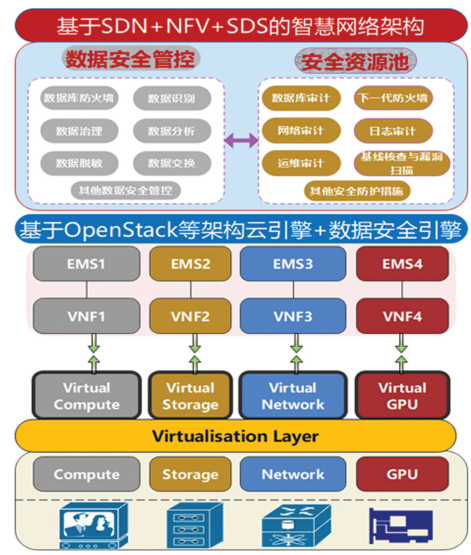

图 4 平台体系架构

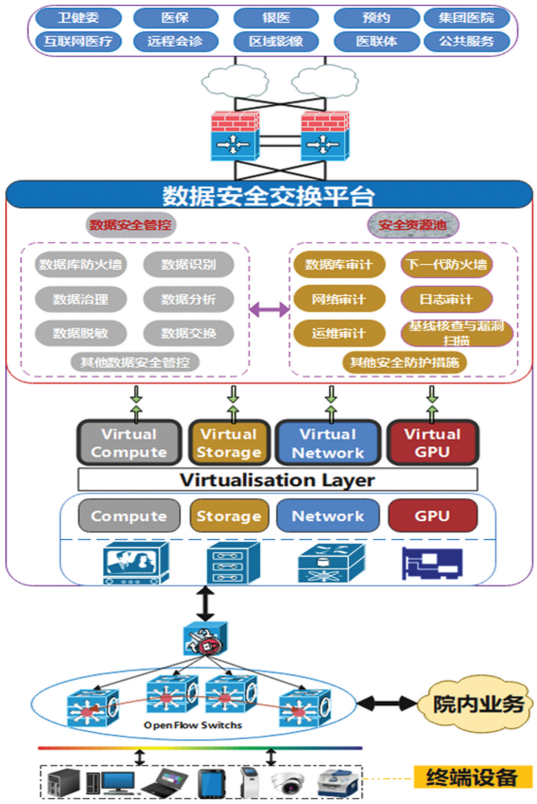

图 5　数据安全交换平台网络拓扑示意图

4　建设内容及实现

4.1　平台底层架构

在内外网业务边界构建数据安全交换平台，实现内外网之间的安全隔离，让内外网交互的业务数据经过平台进行精细化管理和清洗。平台通过云化方式实现，确保平台在性能上的弹性扩容；且平台底层具备通用性和开放性，确保后期更多安全功能的合入和更广泛的三方安全能力兼容。

本平台底层设计是采用超融合架构及 OpenStack 等技术借助通用 X86 服务器硬件为运行载体、以软件为核心构建底层软件与硬件为一体的体系架构，是将计算、安全、GPU、网络及存储等硬件化的资源进行统一而全面的虚拟化，实现整个平台资源动态分配调度、资源高可用与灵活易扩展、资源服务流程易编排等能力，提供了高效、稳定、动态、可靠的底层运行环境[13-18]。

4.2　平台管理要求

建立具有统一门户、统一权限、统一界面的平台管理端，通过联动各安全组件，利用算法进行 AI 智能分析经过元数据治理形成统一的数据标准，在与对外业务进行交互时其数据需根据算法、自定义规则实现对其静态、动态的脱敏处理后方可放行，从而有效保障数据全生命周期防护，以及数据的安全性、隐私性，避免数据外泄而到导致不必要的麻烦。平台管理模式：(1)统一资源管理模式，根据不同业务需求进行横向和纵向扩展，避免因运算速度、内存容量、存储带宽等性能瓶颈原因导致业务中断；(2)统一安全资源联动模式，可根据业务中出现的安全风险能够实现联动发现及阻断，提高安全资源的利用率，实现全局安全防护；(3)统一运维管理中心，可对平台中的所有组件、策略、管理、日志进行管控，并采用统一汇总模式提供业务、安全等相应地风险；(4)智能化控制策略管理能力，根据实际业务进行建模，构建安全组件的策略、防护等 AI 自主化学习，实现无须人为干预的自动化安全防御措施，达到智能化管理能力。

4.3　安全管控设计

安全组件采用分布式部署方式将平台纵深至内部网络，建设涵盖边界安全、主机安全、通信安全、安全审计等组件，满足网络安全防御能力和接入单位(或用户)强身份认证、数据访问动态访问控制、高级威胁发现等安全能力，能抵御常规网络攻击、蠕虫传播、应用层攻击、数据库攻击等，并能结合安全大数据技术和沙箱技术识别网络中的高级威胁、未知位置，通过组件间的联动技术实现 AI 自主分析网络风险与自动阻断未知安全威胁[19-20]。同时实时采集各域安全组件的安全风险事件，基于安全分析模型根据事件的风险类型与威胁程度进行自主动态感知与防护，通过不断完善与更新模型建立自愈型统一安全防护策略中心，对整个平台安全运行进行运维管理。所有安全组件能力被平台统一集成，可通过 API、Open Flow 流表定义、统一控制数据库等多种形式进行数据采集及安全策略下发，实现覆盖医院整网的、技术领先的安全享交换平台。

基于平台安全基础上建立数据安全管控中心，提供数据分析、数据防泄露、数据脱敏、数据加密等多种安全防护手段，对数据全生命周期的过程中进行状态监控，并对整个数据安全过程风险分析与防护。所有数据安全能力被平台统一集成，同时与各安全组件之间无缝联动，实现实时监测、分析、提取、阻断异常数据传输等功能。当前本院自主设计的平台安全组件主要有以下几部分组成，其组件架构见图 6。

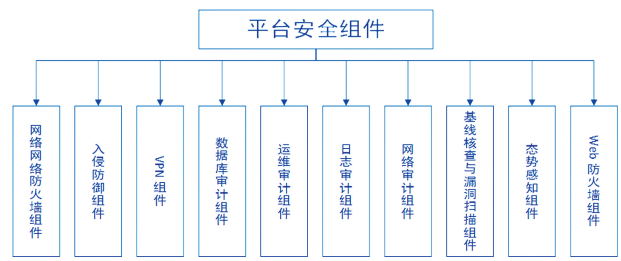

图 6　平台安全组件架构

4.4　元数据集成与治理应用

通过对元数据汇聚整合、提纯加工，让数据服务可视化、将临床业务生产资料转变为数据生产力，同时数据生产力反哺临床，不断迭代循环，让数据驱动决策，提供运营数据价值。其不仅有助于优化现有临床业务，更可助力新业务的创新，同时能提供精细化

运营，打造持续增值的数据资产，同时采用数据集成与治理方式构建边界医疗数据交互的统一数据标准与规范。建立基于算法的数据模型，利用 AI 智能算法分析实现自动进行数据治理、清洗，建立清晰的数据目录、数据关联，有效梳理整理出数据资产、数据目录，理清数据的含义、存储及所属信息等，具备能自动联动平台内其他安全组件，实现数据安全管理贯穿于数据集成与治理的整个过程，提供对隐私数据的加密、脱敏、模糊 化处理、数据库授权监控等多种数据安全管理措施，全方位保障数据的安全运作。元数据集成治理架构见图 7。

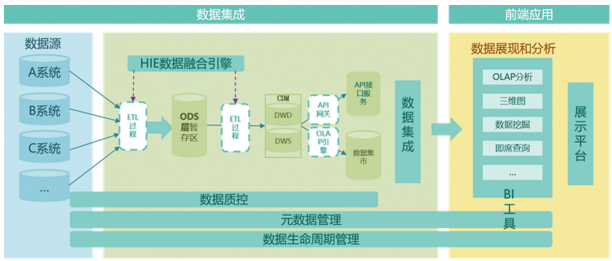

图 7 元数据集成治理架构

4.5 5G 网络支持与优化

网络是基础，平台是核心，安全是保障，传输网络是系统稳定运行的关键环节之一，因此，本设计中传输将采用 5G 网络，利用 5G 技术实现支持不同场景的个性化需求，建立灵活、随需而变的 IT 服务化核心网架构。5G 网络具有高速率、大容量、低时延及核心网全面云化的特点[9]，同时在网络切片方面，通过统一编排可以将 5G、NB-IOT、光网、云资源池等封装为统一的切片，同时叠加本院自主设计的后勤综合管理平台，为本院后勤信息化提供全新的差异化服务。5G 网络总体架构见图 8。

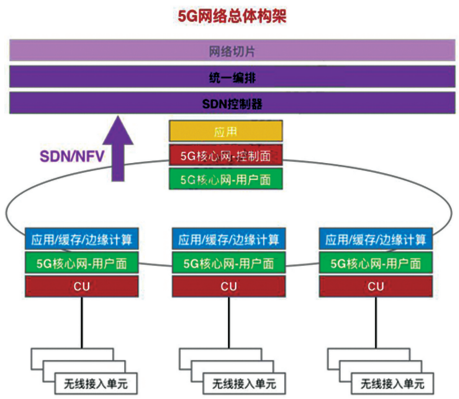

图 8 5G 网络总体架构

4.6 物联网传输支持与优化

物联网是国家新基建中涉及新一代信息技术中的重要部分之一，但准确来说其核心与基础仍旧是借助现有互联网，其是在当前互联网架构与体系的基础上进行“无限”与“泛在”的延伸和扩展。物理网有着“泛互联”的特征，可以通过 X-RFID、LoRa、ZigBee、蓝牙和 5G 等传输技术与各类先进的传感设备按照约定协议，将对人、机、物和事件等互联互通，实现对“万事万物”的识别与定位，同时可追溯、可管控的智能应用和管理，从而构建一个智慧化的万物互联传输网络[8]。物联网建设见图 9。

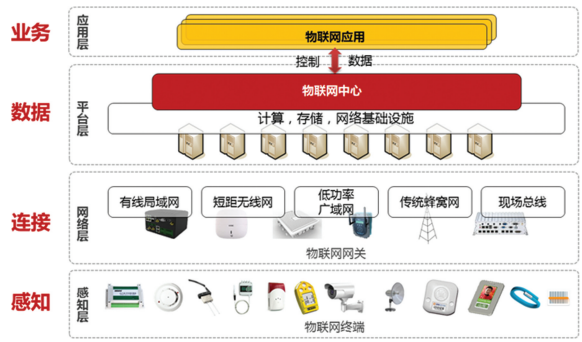

图 9 物联网建设

5 建设成效与意义

5.1 功能快速部署与拓展

依托于云安全平台的安全技术整合能力，平台所有安全防护能力须具备统一一体化交付能力，参照国家《网络安全法》、“等级保护制度”等相关规定与技术参照标准指导本院信息网络安全建设[10]，在平台内部通过安全组件按需选配方式即可快速具备业务的安全防护能力，无须获取某项安全技术能力时可按需对不同安全产品进行单独的采购、配置、授权等。同时满足未来针对智慧医院相关建设、电子病历及互联互通评级的时候，可与时俱进，根据新政策要求进行相应安全组件的弹性拓展和升级，无须采购硬件设备进行堆砌。

5.2 多源异构与松耦合架构

在数据安全交换平台设计中不仅涵盖原有安全能力与第三方安全生态能力，采用开放式业内标准接口，支持多种数据接入协议，多源异构，全量采集，兼容国内主流安全厂商、数通厂商与服务商的安全组件，第三方组件可快速集成至平台中，通过平台强大的融合性、包容性打通数据与管理瓶颈，全面提升安全能力[21-22]。

5.3 运维管控统一与全面

平台采取组件分布式部署，通过建立统一的安全组件管理体系负责平台内部组件及控制、控制数据的统一管理，简化网络架构的同时提升管控维度及效率。该体系可根据自身业务场景定义安全服务组件，也可根据不同业务阶段的需求组合安全服务，简单高效。

5.4 数据融合技术与标准

平台内组建数据治理、数据采集、分类等数据安全相关组件，融合大数据技术架构，可根据业务需求实现数据安全分析建模和多维度态势展示。在基于业务敏感数据自动发现、数据分级分类、数据透明加密、业务脆弱性检测、减少平台性能和业务损耗开销

等方面，加强对敏感数据识别、追踪，利用内容识别、UEBA、机器学习，利用内容识别、UEBA、机器学习等技术，及时发现数据所承载的系统、业务、网络、终端中的安全威胁，提前做好防范措施，让数据防护可视化，安全防范透明化。

5.5 “云一网一端”全层次闭环可视化立体防护

数据交换安全平台建设考虑主动防护和闭环安全，打造集检测、防御、响应与处置为一体的全闭环网络信息安全防护体系，变被动防御为主动防御，构建云一网一端（云，海量云端数据共享；网，保障边界安全；端，保障终端接入安全）多维度网络安全架构。同时需兼具智能协同，持续进化，运用人工智能技术，解决黑白名单、特征、规则无法解决的单一规则问题，以 AI 驱动防御、检测、响应，提升闭环安全的自动化水平，以数据、算法、人驱动模型迭代，使 AI 不断适应新威胁、新形势。

6 结　语

智慧医疗数据交换平台是本院网络信息安全建设中的重中之重，是实现院内外，医院内各部门之前信息联动、交换、共享的基础，其不仅有助于医院信息安全与隐私保护，更有利于本单位系统内同其他医疗单位之间的医疗数据互联互通。当前，本院智慧医院数据中的各系统仍需逐步建设和完善，智慧医院发展之路也需不断探索与实践。将来智慧医院得发展必将会推动卫生医疗行业的发展，真正实现“智慧”二字，不仅能为医院提供智慧管理、智慧教学和智慧后勤等优质服务，同时还能为广大患者提供更为便捷、人性化、个性化的智慧医疗服务，切实助力我国卫生健康事业发展。

参考文献

[1] 叶红.“健康中国 2030”背景下我国中医医疗服务的发展研究[J].中医药管理杂志，2021，29(12)：226-227.

[2] 张菀航.共建共享“互联网＋医疗健康”新生态[J].中国发展观察，2018(9)：50-52.

[3] 张洲.基于物联网的智慧农业系统设计及实现[D].成都：电子科技大学，2019.

[4] 石丽梅，朱又敏，郑颖，等.基于移动通信技术的 5G 时代核心网架构研究[J].无线互联科技，2019，16(12)：7-8.

[5] 李可欣，王兴伟，易波，等.智能软件定义网络[J].软件学报，2021，32(1)：118-136.

[6] 张之阳.基于 SDN 的云数据中心 DDoS 攻击防御方法研究[D].杭州：浙江工商大学，2019.

[7] 冯淼淼.SDSN 中 OpenFlow 协议扩展及联合资源分配模型研究[D].西安：西安电子科技大学，2017.

[8] 傅宇.浅析基于 5G 的物联网应用关键技术[J].中国新通信，2019，21(8)：17.

[9] 关勇，张佳军.基于 5G 的新一代广电网络架构研究[J].广播与电视技术，2018，45(12)：36-41.

[10] 于臣军.从等级保护角度浅谈公安视频网安全建设[J].中国公共安全，2018(7)：178-179.

[11] 胡尧，龚文杰，曾振，等.软件定义网络安全技术研究[J].电子世界，2020(1)：103.

[12] 周晨烁.软件定义网络在医院中的应用及其安全性研究[D].山东中医药大学，2019.

[13] 章岐贵，黄海，汪有杰.基于零信任的软件定义边界安全模型研究[J].信息技术与信息化，2020(11)：92-94.

[14] 王世玲，张江，谢敬锐，等.基于软件定义网络的大型企业安全内网设计[J].网络安全技术与应用，2020(7)：18-19.

[15] 郑忠斌，黎聪，王朝栋.一种面向软件定义网络的安全态势感知方法[J].信息技术与网络安全，2020，39(4)：5-12.

[16] 张倩.软件定义网络安全优势和相关问题[J].电子技术与软件工程，2020(7)：233-234.

[17] 张鉴，唐洪玉，刘文韬，等.面向云网融合的电信网安全防护体系参考架构[J].电信科学，2020，36(5)：10-15.

[18] 董仕.软件定义网络安全问题研究综述[J].计算机科学，2021，48(3)：295-306.

[19] 李波，侯鹏，牛力，等.基于软件定义网络的云边协同架构研究综述[J].计算机工程与科学，2021，43(2)：242-257.

[20] 孙浩博，王海涛.软件定义网络的安全解析及其在安防行业中的应用[J].中国安防，2021(Z1)：112-118.

[21] 张少芳，王剑钊，刘延锋.基于 SDN 的云数据中心安全防护技术研究[J].科技风，2021(3)：70-71.

[22] 安进朝.基于软件定义网络的技术与安全体系探索[J].网络安全技术与应用，2021(1)：6-7.

（收稿日期：2021-03-11　修回日期：2021-06-27）