



开放科学
(资源服务)
标识码
(OSID)

科技信息孪生系统分层防御体系研究

刘勇^{1,2}

- 福建省科学信息技术研究所 福州 350003;
- 福建省信息网络重点实验室 福州 350003

摘要: [目的/意义] 科技信息孪生系统因虚实交互复杂、数据敏感, 面临严峻跨域攻击与隐私泄露风险, 构建适配防御体系可为后续研究提供参考。[方法/过程] 通过文献调研与概念分析, 明确科技信息孪生系统的内涵特征, 提炼出科技信息多元融合、信息传递的分层实时适配性、物理—虚拟闭环协同、系统架构协同复杂四方面特征, 以及用户需求、网络架构、数据类型、调整能力、技术选型、法律与合规性等六个影响因素, 进而分析防御需求与发展趋势。[结果/结论] 提出在“虚实交互—威胁响应—策略优化”循环中实现动态防护, 从网络边界、信息收集与分析、数据保护、应用与服务、跨域协同防御五维度构建框架。该框架突破传统模式, 打破虚实防护壁垒, 融入动态自适应机制, 形成多维度多层次立体防御体系。

关键词: 科技信息孪生系统; 防御体系; 网络技术; 信息监测; 跨域

中图分类号: G35; TP391

Research on Hierarchical Defense System of Science and Technology Information Twin System

LIU Yong^{1,2}

- Fujian Institute of Scientific And Technological Information, Fuzhou 350003, China;
- Fujian Key Laboratory of Information Network, Fuzhou 350003, China

Abstract: [Objective/Significance] Due to the complex virtual-physical interactions and the sensitivity of data involved, sci-tech information twin systems face significant risks of cross-domain attacks and privacy breaches. Developing an adaptive defense framework can offer valuable guidance for future research. [Methods/Processes] Through literature review and conceptual analysis, this study defines the essential characteristics of sci-tech information twin systems, identifying four core features: multi-source integration of technological information, hierarchical real-time adaptability in information transmission, closed-loop collaboration between physical and virtual systems, and coordinated complexity within system architectures. It also identifies six key influencing factors: user requirements, network architecture, data types, adaptability, technology choices, and legal

基金项目 福建省科技计划项目“区域科技创新数据监测技术研究——以福建省为例”(2024R1008008)。

作者简介 刘勇(1975-), 通信作者, 硕士, 高级工程师, 主要研究方向为信息资源管理、科技情报研究、科研管理, E-mail: 813723857@qq.com。

引用格式 刘勇. 科技信息孪生系统分层防御体系研究[J]. 情报工程, 2025, 11(5): 36-47.

and regulatory compliance. Based on these, the study further analyzes defense demands and development trends. [Results/Conclusions] This paper proposes the implementation of dynamic protection in the cycle of “virtual-real interaction-threat response-strategy optimization”, and constructs a framework from five dimensions: network boundary, information collection and analysis, data protection, application and service, and cross-domain collaborative defense. This framework breaks through the traditional model, removes the barriers between virtual and real protection, incorporates a dynamic self-adaptive mechanism, and forms a multi-dimensional, hierarchical and three-dimensional defense system.

Keywords: Science and Technology Information Twin System; Defense System; Network Technology; Information Monitoring; Cross-domain

引言

科技信息孪生系统作为智能平台，是科学研究与技术创新的关键基础设施。在新技术发展和多样化需求的驱动下，全球网络安全形势日趋严峻，传统基于边界防护的防御体系已难以有效应对科技信息孪生系统所面临的新型安全威胁^[1-4]。CheckPoint《2025年网络安全报告》显示，全球网络攻击数量同比显著增长44%，攻击者利用生成式人工智能（GenAI）加速攻击进程，导致信息窃取程序攻击量暴涨58%^[5]。IBM《2024年数据泄露成本报告》进一步指出，高达70%的企业因安全漏洞而遭受严重运营冲击，且安全漏洞从被发现到完全控制的平均耗时达272天。为了应对此类挑战，在国家战略的引导和推动下，我国科技信息界日益重视信息监测技术和网络安全环境治理，并积极支持数字孪生技术与其他智能技术等新技术的创新应用，旨在强化信息采集、分析和处理，从而有效保障科技信息系统安全运行。

1 科技信息孪生系统内涵与特征

科技信息孪生系统的相关研究由来已久，不过，其内涵和特征研究还有待深入。笔者将

基于相关学者研究，归纳出科技信息孪生系统的内涵与特征，为科技信息孪生系统的防御体系构建确定研究范围。

1.1 科技信息孪生系统内涵

将科技信息服务生态系统与数字孪生紧密结合，对科技信息孪生系统内涵进行阐述，反映实体全生命周期的过程。

1.1.1 相关理论概述

马费成等^[6]将科技信息资源定义为科技活动中形成的，以科技信息为核心，涵盖信息主体、内容及技术设施等要素的集合。刘佳等^[7]提出科技信息服务生态系统是以科技信息资源和技术为基础，以服务机构为主导，各类主体与用户共同参与，以支持科技创新和科学决策为目标，以价值共创为核心，通过信息流驱动多流联结形成的开放、复杂、动态调节、共生竞合的生态系统，是相关系统的数据与服务生态根基。

数字孪生概念由Grieves^[8]于2003年提出，为“与物理产品等价的虚拟数字化表达”，含实体、虚拟产品及连接的三维模型。Glaessgen等^[9]将其定义为集成多物理量、多尺度、多概率的仿真过程，基于物理模型构建完整映射的

虚拟模型，利用历史及实时数据刻画物理对象全生命周期。庄存波等^[10]认为数字孪生是利用数字技术对物理实体特征、行为等进行描述和建模的过程和方法。Tao等^[11]提出数字孪生包含物理实体、虚拟模型、服务系统、孪生数据和连接五维结构，是连接物理与信息世界的智能技术^[12]。

可见，孪生系统核心是虚实映射，即通过数字化技术为物理实体构建数字镜像，借助实时数据同步、动态模拟及双向交互，实现对物理实体的监控、分析、预测与优化。

1.1.2 科技信息孪生系统基本概念

基于既有研究，科技信息孪生系统的根本属性是“物理实体的数字化表征体”，其关键作用在于将科技信息服务生态系统所蕴含的信息价值精确投射到物理领域，并借助反向反馈机制对生态系统的动态优化过程形成支撑。二者呈现“中枢与末梢”的协同关系：生态系统作为信息处理与资源调度的软性中枢，科技信息孪生系统则作为实体感知与决策执行的硬性末梢，共同支撑科技活动实现“数据驱动”与“虚实协同”的运行模式。

(1) 内涵

科技信息孪生系统是基于数字孪生技术构建的科技信息管理全生命周期虚拟化智能系统，其核心特征体现为“虚实融合”与“软硬协同”：在硬性与实体维度，通过高精度数字化手段，对图书馆、科研院所信息中心等科技信息管理实体及其关联的物理设备、人员等硬件要素进行动态适配的虚拟映射建模，实现异构硬件要素的智能感知与全域互联；在软性与虚拟维度，深度集成多源异构数据（包括设备运行状态、

硬件传感数据等硬性实体数据，以及服务流程交互记录、知识资源存取轨迹、科研需求反馈等软性非实体数据），依托实时数据流动与智能分析技术，构建物理管理场景与虚拟镜像的双向实时交互机制，最终通过虚实协同优化达成科技信息资源的精准配置与服务流程的动态迭代。其基本构成如图1所示。

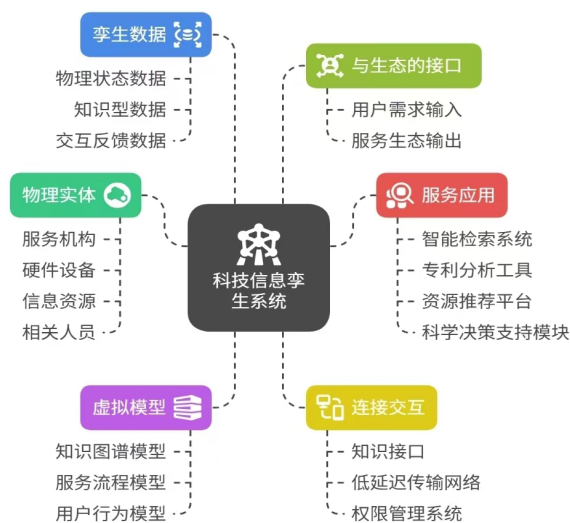


图1 科技信息孪生系统要素构成

(2) 功能及要素

该系统能实现异构硬件的智能感知与全域互联、多源数据的深度融合与分析，构建物理场景与虚拟镜像的双向实时交互机制，从而达成科技信息资源的精准配置、服务流程的动态迭代，提升资源配置效率，增强科技信息服务生态系统的动态适应性与创新赋能效能，支撑科技活动实现“数据驱动”与“虚实协同”。

该系统具体包含五方面要素：

(1) 物理实体。作为系统源头载体，涵盖服务机构、物理设备、科技信息资源及参与主体。其异构性与动态性，决定了虚拟映射的复杂性

与适应性需求。

(2) 虚拟模型。物理实体的动态镜像，是融合几何、物理、行为、知识建模的多维度复合模型，并非简单数字化复制，能实时响应物理实体变化并仿真推演，实现智能化数字化表征。

(3) 孪生数据。系统的“智能基因”，集成物理实体实时数据、虚拟模型交互数据及外部关联数据，经处理与分析后，驱动虚拟模型迭代与物理实体优化，形成数据闭环。

(4) 连接交互。虚实协同的“神经中枢”，借助物联网等技术构建双向通信链路，实现全要素互联、数据传输集成及实时交互控制，是虚实融合的核心技术支撑^[13]。

(5) 服务应用。系统价值输出的核心载体，基于虚实融合的数据与模型开发智能化管理工具，为科技信息管理提供功能支持，推动服务模式从“被动响应”向“主动创新”转型。

1.2 科技信息孪生系统特征

基于科技信息孪生系统的内涵，结合数字孪生系统核心功能及科技信息动态知识本质，其特征可归纳为科技信息的多元融合性、信息传递的分层实时适配性、物理—虚拟的闭环协同性、系统的协同复杂性，这四大特征构成其区别于传统系统的核心优势^[14-16]。

(1) 科技信息的多元融合性

科技信息的多元融合性本质是“显性知识与隐性知识的协同转化”。传统系统仅处理文献文本等显性知识，该系统通过关联建模技术，将二者整合为可动态交互的知识网络，既实现科研数据等显性信息的结构化呈现，又完成科研思路等隐性信息的显性化表达，形成覆盖科

技创新全链条的信息生态。

(2) 信息传递的分层实时适配性

信息传递的分层实时适配性核心是实现科研全周期动态需求与信息时效响应的精准匹配。该系统基于科研“探索—验证—沉淀”全周期特征设计分层策略：探索阶段需高实时性同步实验数据以支撑试错迭代，验证阶段依托可控延时的时效响应保障方案优化的时效与精准，沉淀阶段降低实时性要求聚焦知识关联沉淀，最终精准匹配科研动态需求^[17]。

(3) 物理—虚拟的闭环协同性

突破传统系统“人机二元控制”局限，构建“科研主体—虚拟模型—物理实体”三元互动网络。融合科研主体创造性思维、虚拟模型数据分析能力与物理实体实践验证功能，形成“设计方案—执行反馈—优化反哺”的创新闭环，实现全流程协同。

(4) 系统的协同复杂性

与一般系统“静态拓扑复杂性”有本质区别，其复杂性是有序的结构与规律。通过数据、知识、协作链路多维交织，实现物理设备、科技信息、科研主体协同联动，随科研进程动态进化，服务于科研创新目标，展现高效自适应与自优化能力。

2 相关研究

在科技信息孪生系统安全领域，已有不少研究成果。Lee等^[18]、张霖等^[19]从孪生系统的内涵与特性出发挖掘其本质特征；李欣等^[4]从宏观层面构建防御体系，任乾坤等^[20]构建的网络数字孪生模型强调物理与孪生系统的交互及

基础安全措施；徐波等^[21]构建了数字孪生水利工程网络安全技术风险治理体系；马宇威等^[22]针对网络攻击技术进行安全防御部署，但这些研究均未深度融合网络技术与信息分析流程，无法实现安全技术与信息监测的有机联动。

具体技术应用可分为三类：一是 VonWill-ich 等^[23]、Olade 等^[24] 聚焦技术手段优化，忽视信息获取、分析与技术防护的协同需求；二是 Suhail 等^[25]、Alcaraz 等^[26] 基于区块链强化数据访问安全，却未将信息监测与分析场景纳入技术架构设计；三是针对数字孪生体安全创建、数据加密等环节开展研究^[27-28]，多停留在技术层面，未深入探讨技术与信息协同产生的新型风险及关键环节。

现有研究多侧重网络安全技术的独立应用或信息分析的理论方法，领域协同性不足，网络技术与系统内外的信息收集、分析流程缺乏有效整合，也未建立双向互动的协同防御机制，这导致安全防御体系难以有效识别复杂威胁、实现主动防御。因此，亟需从技术和信息配合的角度出发，建立分层且多维度的防护结构，打破跨领域配合受限的壁垒，精准应对不同阶

段、不同类型的安全威胁。本研究为科技信息系统防御机制的持续完善提供新的思路，提升跨领域的协同防御能力，有效应对新的风险问题，推动智能防御和标准化发展。

3 科技信息孪生系统防御需求及影响因素分析

基于科技信息孪生系统的内涵和特性，系统防御需求可归纳为安全防护、快速响应、协同防御、自适应防御四个方面。基于此，将这些抽象需求转化为可落地的防御策略，并探寻防御影响因素。

3.1 科技信息孪生系统防御需求分析

科技信息孪生系统的防御需求由其固有属性与外部环境共同驱动。因数据密集，需防范敏感数据泄露、篡改；高实时性科研场景要求快速处理数据以保时效；多组件架构和数据交互网络需协同防御；科研需求等要素的动态变化则要求自适应调整。这些需求源于系统数据属性、应用场景和架构特点。科技信息孪生系统的防御需求如图 2 所示。

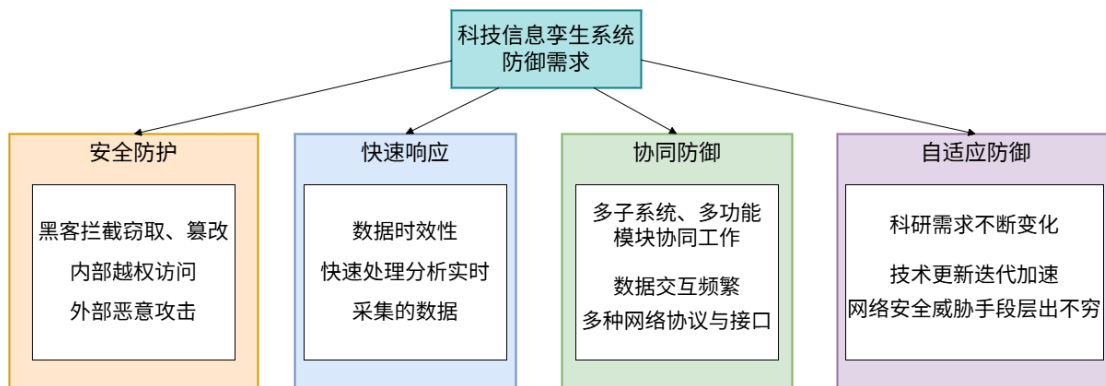


图 2 科技信息孪生系统防御需求分析

结合需求分析，科技信息孪生系统的防御措施正从“被动、单一、静态”的传统防御，向“主动、协同、动态”的新型防御体系转型，核心是让防御能力与系统的数据属性、应用场景、架构特点精准匹配，最终实现“安全与效率”“防护与科研”的协同平衡。

（1）安全防护需求

系统承载科研数据、实验结果及用户隐私等高价值敏感信息，安全性至关重要。数据在传输中可能被黑客拦截窃取或篡改，存储时可能遭遇内部越权访问或外部攻击，例如科研数据泄露会造成知识产权损失，影响成果转化；用户信息被篡改则损害权益并引发信任危机。其防护已从传统“静态边界防护”转向“动态自适应防御”：传统系统依赖固定防火墙和统一加密标准，缺乏对内部授权用户的持续监控，难以应对新型攻击；而该系统防御体系具有“随威胁进化而迭代”的特征，如检测到新型加密破解技术时，会自动切换至更高强度加密协议；发现内部人员通过隐蔽通道传输数据时，会动态收紧权限并新增行为为基线检测。

（2）快速响应需求

在科研与决策支持场景中，数据时效性非常关键，延迟可能导致科研项目延误或决策失误。以实验数据为例，实时处理能帮助科研人员及时调整参数，提升效率。防御模式已从传统“事后追溯型”转向“实时拦截—并行处理型”：传统系统安全防护优先保障数据完整性，采用“先处理数据、后检测威胁”的串行模式，可能因防御流程导致延迟；而该系统防御机制实现“防御与业务的并行协同”，当实验室设备实时上传数据时，边缘节点的轻量化 AI 防御

模块同步进行威胁检测，避免防御成为科研时效性瓶颈。

（3）协同防御需求

系统架构复杂，多个子系统和功能模块协同运作，数据交互频繁，涉及多种网络协议与接口，单一防护技术难以覆盖，零信任架构通过持续身份验证打破传统信任边界，保障访问安全。防御模式从“各模块独立防护”转变为“全域联动的协同防御生态”：传统系统中，物理设备层、虚拟模型层、服务应用层各自部署防御工具，规则互不关联，易形成“防御孤岛”；而该系统通过构建“防御中枢—子系统代理”的星型网络，实现威胁情报实时共享与防御动作跨层同步。

（4）自适应防御需求

系统所处环境动态多变，科研需求变化、技术迭代加速、网络威胁层出不穷^[29]，例如新攻击技术可能使原有策略失效，科研项目调整会改变系统功能与数据需求，导致防护重点转移。防御措施从“预设规则静态防御”转变为“动态学习自适应防御”：传统防御依赖人工预设规则，面对新攻击或系统变化时需手动更新，存在滞后性；而该系统自适应防御构建“威胁感知—模型学习—策略迭代”闭环机制，通过持续采集新型攻击样本、科研场景变化数据，利用机器学习算法实时优化防御模型。

3.2 科技信息孪生系统防御的影响因素

科技信息孪生系统防御体系的构建面临诸多层面的挑战：用户在多元角色下提出的多样化需求加剧了安全性与用户体验之间的平衡困境；复杂网络的拓扑结构扩大了潜在攻击的范

围,使传统防护措施捉襟见肘;需要根据数据的敏感属性进行层次化防护,以避免资源配置失当;动态环境要求防御体系进行自适应调整;新旧技术之间的兼容性问题削弱了防护效果;

数据法规的严格规定要求防御架构不断重构以保持合规。这六个方面的因素共同影响着防御系统的构建。科技信息孪生系统防御的影响因素如图3所示。

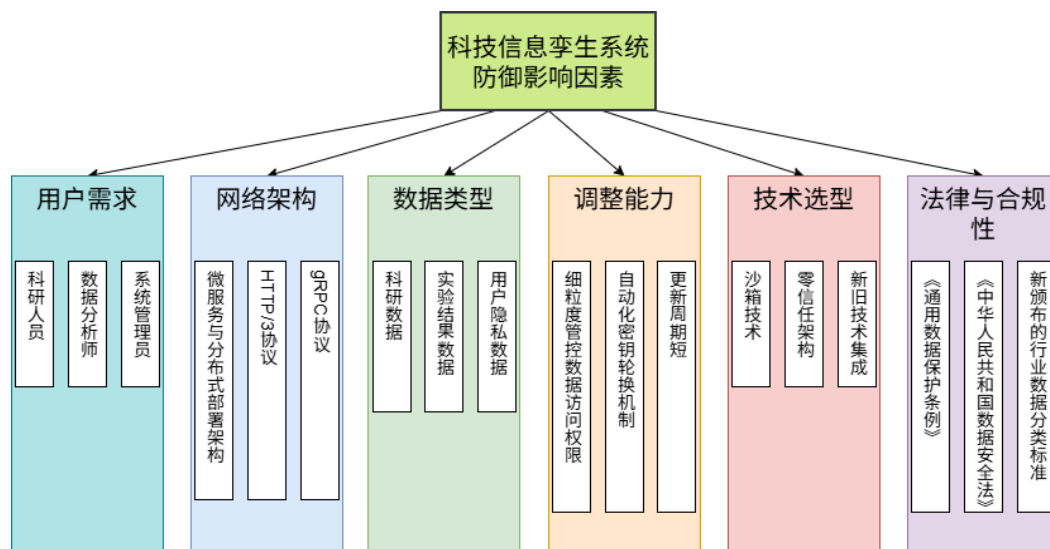


图3 科技信息孪生系统防御影响因素理论模型

(1) 用户需求

科技信息孪生系统服务于科研人员、数据分析师和系统管理员等不同用户群体。科研人员关注数据访问的高效性,倾向于简化验证流程,但这可能带来审批漏洞,增加外部入侵风险。数据分析师强调数据完整性,要求在传输存储环节部署复杂的校验机制,这会引起系统处理延迟。系统管理员为保障系统安全实施严格权限管控,有可能促使用户绕过安全规则使用外部存储设备传输数据。这些用户需求的多样性与安全防护要求之间的矛盾,使得防御体系在平衡安全性与用户体验时面临巨大挑战。

(2) 网络架构

科技信息孪生系统采用微服务架构和分布式部署,其数据交互涉及HTTP/3、gRPC等多

种协议,构筑复杂的异构网络拓扑。在此框架下,传统的基于边界防护的安全策略难以发挥作用。单一模块的安全漏洞可以通过服务网格迅速扩散至整个系统;负载均衡器的配置错误可能导致流量分配不均,造成部分节点过载并暴露服务端口;SDN控制器与防火墙策略的同步延迟,则可能导致恶意流量绕过限速规则^[30-31]。这些架构特性不仅扩展了系统的潜在攻击面,更使得攻击路径难以预测。

(3) 数据类型

科技信息孪生系统所处理的科研数据、实验结果数据及用户隐私数据,因其敏感属性程度各异,故而对应不同的安全防护需求。科研数据作为学术成果的核心载体,其真实性与完整性直接影响科研价值,需采用区块链存证、

Merkle 树校验等技术确保数据不可篡改；对于时效性要求极高的实验结果数据，过度加密可能导致处理延迟，进而影响决策响应速度，因此需采用轻量级加密算法；用户隐私数据则必须遵循最小必要原则，并运用动态脱敏、联邦学习等技术，在保证数据可用性的同时防止隐私泄露。

（4）调整能力

科研需求的持续迭代、技术架构的不断升级以及网络威胁的日益演变，共同要求科技信息孪生系统防御体系具备动态自适应能力。例如，当科研项目从传统数据存储转向 AI 模型训练时，数据访问权限的需求也随之演变，从传统的基于角色的粗粒度控制模式转向基于模型版本的细粒度管控机制。传统 RBAC 模型在此类新型场景下难以满足新需求。此外考虑到量子计算技术有可能破解现有加密算法的风险，若系统缺乏自动化密钥轮换机制，数据机密性将面临重大威胁。

（5）技术选型

在构建防御体系的过程中，传统安全技术（例如防火墙、入侵防御系统）与新兴技术（如零信任架构、区块链存证）的融合遭遇诸多挑战。例如沙箱技术在隔离恶意代码的过程中，若与容器编排系统的资源调度机制不兼容，可能会导致服务响应时间延迟，降低用户体验；零信任架构所强调的“永不信任，始终验证”原则与传统基于信任域的认证机制在逻辑上存在潜在的冲突，未经有效策略映射与接口适配，可能会导致访问控制混乱，增加安全风险。

（6）法律与合规性

在全球范围内，数据保护法规如欧盟的

《通用数据保护条例》（General Data Protection Regulation, GDPR）以及我国的《中华人民共和国数据安全法》，均对科技信息孪生系统的数据处理活动提出了明确要求。随着技术发展，科技信息孪生系统防御体系需要进行持续性的架构重构，以实现安全防护与法律合规的双重目标，避免因违规带来的法律风险与声誉损害。

4 防御体系框架设计

科技信息孪生系统是“开放与闭环的辩证统一”，这种特性与其“虚实融合、动态协同”的本质深度关联。基于此，本文构建涵盖网络边界层、信息收集与分析层、数据保护层、应用与服务层以及跨域协同防御层的多维度多层次防御框架体系，如图 4 所示。该框架既通过跨域协同防御层适配系统的开放性，支持外部主体安全接入与数据共享；又依托各层级的联动机制强化核心闭环，在“虚实交互—威胁响应—策略优化”的循环中实现动态防护，形成与系统特性相匹配的防御逻辑。

与传统防御模式相比，这一框架体系呈现出显著的创新性：传统防御多聚焦于物理空间的单点防护，依赖静态规则和边界隔离，难以应对跨空间、多维度的安全威胁；而该框架以“技术与信息协同”为支撑，以“虚实空间协同防御”为核心，打破物理与虚拟的防护壁垒，通过多层级联动实现从边界到数据、从应用到跨域的全场景覆盖，且融入动态自适应机制，能根据威胁演变和系统变化实时优化防御策略，最终形成“主动感知、智能协同、全域防护”的新型防御格局。

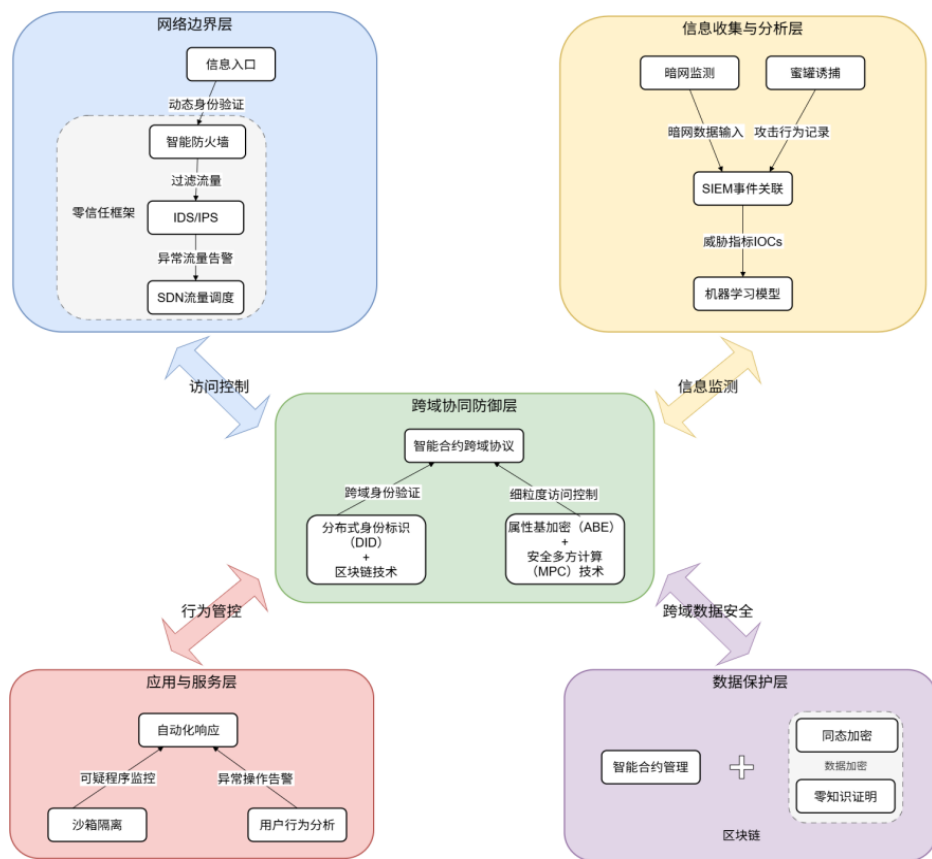


图 4 科技信息孪生系统防御系统框架图

4.1 网络边界层

网络边界层是抵御外部威胁的核心屏障，需适配网络环境复杂、动态及安全稳定需求，结合多传感器布局、动态组网及多时空尺度协同测量理论，以“技术落地+策略迭代”模式构建多层次防护体系。硬件方面，智能防火墙与零信任融合，依托硬件流量过滤与软件策略生成细粒度规则，零信任借 MFA 硬件提升验证强度；智能 IDS/IPS 与 SDN 协同，以硬件加速芯片分析流量，构建基线模型捕捉攻击，IPS 自动处置并同步策略，形成闭环。

策略上，基于用户角色和科研场景构建权限动态调整模型，通过平台实时更新规则实现

“最小权限”柔性落地；建立威胁等级划分标准，结合历史数据与系统负载，通过策略引擎动态调整响应优先级，避免过度防御导致资源浪费。

4.2 信息收集与分析层

信息收集与分析层作为防御体系的“中枢神经”，围绕数据多样性、实时响应需求及主动防御目标，以“硬件设备采集数据+软件模型深度分析”的协同模式构建智能化威胁感知与分析体系。硬件支撑体现在多维度数据采集硬件的部署，包括暗网专用爬虫服务器、流量镜像设备、终端行为采集探针，实现多源数据全量采集；搭建高仿真蜜罐硬件集群模拟科研业务环境，吸引攻击者并通过硬件级日志模块

记录攻击特征，为溯源提供原始数据。

模型方面，基于 SIEM 系统构建多源数据融合分析算法框架，运用 NLP 解析暗网敏感信息，通过 GNN 关联攻击要素还原链路，结合 UEBA 算法识别异常行为；建立与外部的情报共享接口，实时同步科技领域专属威胁情报，结合内部数据通过机器学习迭代优化威胁识别模型，提升研判准确率。

4.3 数据保护层

数据保护层围绕数据类型多样性与隐私合规严格要求，集成实时可靠链路调度技术，以“硬件级加密存储 + 软件化规则管控”的协同模式实现多粒度异构数据融合，构建全流程、立体化的数据安全防护体系^[13]。硬件部署搭载安全加密芯片的区块链节点服务器，将关键数据哈希值写入分布式账本，结合 RAID 冗余技术实现数据物理层面的防丢失、防篡改；采用搭载同态加密加速芯片的服务器和零知识证明专用硬件模块，提升加密运算效率与身份核验安全性。

规则方面，基于区块链平台编写数据全生命周期智能合约，将各环节规则编码为不可篡改的程序代码，自动执行操作并校验合规性；建立科技信息数据分级标准，通过软件平台自动分类标记，针对不同级别数据制定差异化防护策略，实现精细化与柔性化防护。

4.4 应用与服务层

应用与服务层作为用户交互核心枢纽，需契合需求多样性、实时响应及系统稳定性标准，以“硬件级环境隔离 + 软件化流程响应”的协

同模式实现多模态数据与对象行为的语法和语义映射，构建动态交互、自适应控制的安全防护体系。硬件支撑包括部署搭载虚拟化硬件辅助技术的专用沙箱服务器，为可疑程序提供隔离运行环境并监控其行为；搭建基于 Ansible 的自动化运维硬件集群，实现威胁处置命令的快速下发与执行，缩短响应时间。

流程上，建立“事前—事中—事后”全流程响应机制，事前扫描漏洞并制定修复计划，事中按攻击类型执行预设处置流程，事后还原攻击过程并生成安全报告，优化防御策略。

4.5 跨域协同防御层

跨域协同防御层应对复杂网络中系统互操作安全挑战，兼顾动态架构、跨域数据共享及合规约束，基于分布式协同控制理论，以“硬件互联 + 软件协同”建立一体化防护体系。硬件方面，为跨域用户配备 DID 硬件钱包存储身份凭证，部署 ABE 服务器支撑细粒度访问控制；建设专用安全通信网，借加密隧道隔离传输，在边缘节点预处理数据，降低核心网络风险。

机制方面，基于区块链平台编写跨域协同智能合约，固化协同规则并自动同步攻击信息、更新防御策略，动态调整参与方信任等级；建立跨域安全联盟，制定统一标准实现信任互通。

5 结论与展望

本文构建了一个科技信息孪生系统的分层防御体系，该体系包含网络边界层、信息收集与分析层、数据保护层、应用与服务层及跨域协同防御层。各层级通过智能防火墙与零信任

框架过滤恶意流量、利用暗网监控与蜜罐技术感知潜在威胁、依托区块链与加密技术保护数据隐私、借助沙箱与自动化响应机制强化终端安全以及基于分布式身份管理与智能合约实现跨域协同,有效应对科技信息孪生系统数据密集、架构复杂等特性带来的安全挑战,提升了主动防御能力与跨域协同效率。

未来研究需进一步探索生成式 AI 在攻击预测与防御策略动态生成方面的应用;加强对量子计算攻击、供应链攻击等新型威胁的防御技术研究;深化跨系统数据共享与策略联动机制以优化跨域协同效果;通过模拟真实攻击场景对所构建的防御体系进行实战化验证,从而持续迭代优化各层级技术组合与协同流程。

参考文献

- [1] 毛竞争,胡潇锐,徐庚辰,等.数字孪生在工控安全中的应用进展综述[J].计算机工程,2025,51(2): 1-17.
- [2] 冯瀚锐,谢安明,高健博,等.数字孪生城市基础设施安全保障体系研究[J].信息安全研究,2024,10(11): 997-1003.
- [3] 李辉,曾文,刘彦君,等.面向科技安全的科技情报监测与分析系统构建研究[J].情报理论与实践,2021,44(6): 98-104.
- [4] 李欣,刘秀,万欣欣.数字孪生应用及安全发展综述[J].系统仿真学报,2019,31(3): 385-392.
- [5] 陶飞,刘蔚然,刘检华.数字孪生及其应用探索[J].计算机集成制造系统,2018,24(1): 1-18.
- [6] 马费成,宋恩梅,赵一鸣.信息管理学基础(第三版)[M].武汉:武汉大学出版社,2018.
- [7] 刘佳,邵诗雅,彭鹏.科技信息服务生态系统健康评价体系构建与实证研究[J].图书情报工作,2018,62(11): 88-96.
- [8] GRIEVES M. Digital twin: manufacturing excellence through virtual factory replication[EB/OL]. (2014-03-12) [2025-05-20]. http://www.aprison.com/library/Whitepaper_Dr_Grieves_DigitalTwin_ManufacturingExcellence.php.
- [9] GLAESSGEN E, STARGEL D. The digital twin paradigm for future NASA and US Air Force Vehicles[C]// Proceedings of the 53rd Structures Dynamics and Materials Conference (Special Session on the Digital Twin). AIAA, 2012: 1-14.
- [10] 庄存波,刘检华,熊辉,等.产品数字孪生体的内涵、体系结构及其发展趋势[J].计算机集成制造系统,2017,23(4): 753-768.
- [11] TAO F, ZHANG M. Digital twin shop-floor: a new shop-floor paradigm towards smart manufacturing[J]. IEEE Access, 2017(5): 20418-20427.
- [12] 刘蔚然,陶飞,程江峰,等.数字孪生卫星:概念、关键技术及应用[J].计算机集成制造系统,2020,26(3): 565-588.
- [13] 陶飞,程颖,程江峰,等.数字孪生车间信息物理融合理论与技术[J].计算机集成制造系统,2017,23(8): 1603-1611.
- [14] 陶飞,刘蔚然,张萌,等.数字孪生五维模型及十大领域应用[J].计算机集成制造系统,2019,25(1): 1-18.
- [15] 何劲,王曰芬,傅柱.动态情报研究模式重构及实践[J].情报理论与实践,2023,46(10): 54-60.
- [16] 蒲云强,唐川,徐婧,等.基于大语言模型的科技动态情报感知研究[J].情报理论与实践,2025,48(2): 11-20.
- [17] 孔繁超.基于数字孪生技术的智慧图书馆空间重构研究[J].情报理论与实践,2020,43(8): 146-151.
- [18] LEE J, BAGHERI B, KAO H-A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems[J]. Manufacturing Letters, 2015, 3(1): 18-23.
- [19] 张霖,周龙飞.制造中的建模仿真技术[J].系统仿真学报,2018,30(6): 1997-2012.
- [20] 任乾坤,熊鑫立,刘京菊,等.网络空间安全中的数字孪生技术研究[J].系统仿真学报,2024,36(8): 1944-1957.
- [21] 徐波,王昕.数字孪生水利工程网络安全风险分析

- 和保障体系 [J]. 人民长江, 2023, 54(11): 242-250.
- [22] 马宇威, 杜海涛, 粟粟, 等. 基于数字孪生的 5G 网络安全推演 [J]. 计算机工程与应用, 2024, 60(5): 291-298.
- [23] VON WILLICH J, FUNK M, MÜLLER F, et al. You invaded my tracking space! Using augmented virtuality for spotting passersby in room-scale virtual reality[C]// Proceedings of the Designing Interactive Systems Conference (DIS), San Diego, 2019: 487-496.
- [24] OLADE I, FLEMING C, LIANG H N. BIOMOVE: biometric user identification from human kinesiological movements for virtual reality systems[J]. Sensors, 2020(20): 2944.
- [25] SUHAIL S, HUSSAIN R, JURDAK R, et al. Trustworthy digital twins in the industrial Internet of Things with blockchain[J]. IEEE Internet Comput, 2021, 26: 58-67.
- [26] ALCARAZ C, LOPEZ J. Digital twin: a comprehensive survey of security threats[J]. IEEE Commun Surv Tutor, 2022(24): 1475-1503.
- [27] BÉCUE A, FOURASTIER Y, PRACA I, et al. Cyber-Factory#1-securing the industry 4.0 with cyber-ranges and digital twins[C]// Proceedings of the IEEE International Workshop on Factory Communication Systems (WFCS), Imperia, 2018: 1-4.
- [28] WU J Y, GUO J K, LV Z H. Deep learning driven security in digital twins of dronenetwork[C]// Proceedings of the IEEE International Conference on Communications, Seoul, 2022: 1-6.
- [29] 隆毅. 高校图书馆虚拟社区孪生空间的信息安全建设 [J]. 福建电脑, 2022, 38(2): 70-72.
- [30] 隆毅. SDN 架构的高校图书馆虚拟社区 [J]. 福建电脑, 2020, 36(5): 99-101.
- [31] 李曼, 周华春, 徐琪, 等. 面向 SDN 的攻击流量分配与负载均衡机制 [J]. 通信学报, 2025, 46(3): 74-93.