

# 技术视角下网络空间信任体系模型及发展研究

孙帅<sup>1</sup>, 张蕾<sup>1\*</sup>, 胡春卉<sup>1</sup>, 傅首清<sup>1</sup>, 卿昱<sup>1</sup>, 崔勇<sup>2</sup>

(1. 中关村实验室, 北京 100094; 2. 清华大学计算机科学与技术系, 北京 100084)

**摘要:** 随着网络空间的边界不断扩张, 由信任缺失引发的安全事件逐年增加, 网络空间信任体系面临严峻挑战, 目前研究多聚焦于宏观政策研判及信任模型的应用探索, 对可信发展需求与特征要素的系统性探究相对不足。为此, 本文首先梳理了世界各国网络空间信任的政策演进过程, 分析了信任体系模型发展需求。在此基础上, 从通信层、网络层、系统层、应用层构成的网络空间技术体系出发, 逐层剖析各层面临的信任问题及应对技术, 提出一种基于技术视角的网络空间信任体系模型框架, 凝练出网络空间信任应具备的五大核心功能特征: 身份认证、授权管理、责任认定、数据可信、供应链与服务可信。为进一步验证模型的适用性, 选取了极端条件下网络空间、大模型、数据流通及车联网四个典型场景, 深入分析信任风险与关键技术的应对路径。最后, 提出构建我国网络空间可信生态的发展建议, 为相关政策制定与技术架构设计提供理论支撑。

**关键词:** 网络空间信任体系; 技术模型; 核心功能特征; 零信任; 场景验证

**中图分类号:** TP393.08 **文献标识码:** A

## Model and Development of Cyberspace Trust System from a Technical Perspective

Sun Shuai<sup>1</sup>, Zhang Lei<sup>1\*</sup>, Hu Chunhui<sup>1</sup>, Fu Shouqing<sup>1</sup>, Qing Yu<sup>1</sup>, Cui Yong<sup>2</sup>

(1. Zhongguancun Laboratory, Beijing 100094, China; 2. Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

**Abstract:** With the continuous expansion of cyberspace boundaries, trust-related security incidents are increasing annually, posing severe challenges to the cyberspace trust system. However, current research mostly focuses on macro-policy analysis and the application exploration of specific trust models, with insufficient systematic exploration of the developmental requirements and characteristic elements of trustworthiness. To address this gap, this study reviews the policy evolution trajectories of cyberspace trust frameworks across nations, analyzing the developmental demand for trust system models. Subsequently, we propose a model framework for the cyberspace trust system from a technical perspective, grounded in the cyberspace technological architecture comprising the communication, network, system, and application layers. Through a layer-by-layer analysis of trust challenges and corresponding mitigation techniques, the study further identifies five core functional characteristics essential for cyberspace trust: identity authentication, authorization management, accountability, data trustworthiness, and supply chain and service trustworthiness. To validate the model's applicability, we conduct an in-depth analysis of trust risks and key technical countermeasures across four representative scenarios: extreme-condition cyberspace, artificial intelligence, data flows, and the Internet of Vehicles. Furthermore, recommendations are proposed to support the development of China's trustworthy cyberspace ecosystem, providing theoretical foundations for policy

**收稿日期:** 2025-08-18; **修回日期:** 2025-10-20

**通讯作者:** \*张蕾, 中关村实验室副研究员, 研究方向为网络安全、网络优化等; E-mail: zhanglei@zgclab.edu.cn

**资助项目:** 中国工程院咨询项目“网络空间安全新技术新应用风险研究”(2023-JB-13); 中国科协战略发展部委托项目“新技术变革对网络空间安全态势的影响及对策研究”

**本刊网址:** sscac.engineering.org.cn

formulation and technical architecture design.

**Keywords:** cyberspace trust system; technical model; core functional characteristics; zero trust; scenario validation

### 一、前言

网络空间的安全、稳定与繁荣发展不仅关乎国家和社会稳定，对全球发展也具有深远意义。然而，过去二十多年来，伴随着网络空间边界的持续拓宽、量子计算等新兴技术的不断涌现以及人工智能、物联网等新技术的广泛应用，网络空间信任风险显著增多，给国家和社会治理带来前所未有的挑战<sup>[1]</sup>。2022年，以DigiCert等为代表的主流证书颁发机构（CA）集中吊销了俄罗斯政府和金融机构网站的3000余张证书，导致俄罗斯政府服务平台、银行等重要网站因证书失效而无法访问，严重扰乱了国家关键领域的正常秩序<sup>[2]</sup>。

在当前网络空间安全形势日益严峻的背景下，如何构建更加安全可靠的网络空间信任体系，以维护整体可信生态，已成为产业界和学术界共同关注的焦点。我国在2006年发布的《关于网络信任体系建设若干意见的通知》中，将网络信任体系界定为以密码技术为基础，以法律法规、技术标准和基础设施为主要内容，以解决网络应用中身份认证、授权管理和责任认定等为目的的完整体系<sup>[3]</sup>，然而现阶段网络空间信任体系的定义仍不清晰。网络和空间网络的定义有一定区别，根据ISO/IEC 61158-1:2023对网络的定义可知，网络是由通信介质、连接器、中继器、路由器、网关等元素构成的通信设备集合，通过特定协议实现节点间的互联<sup>[4]</sup>。而ISO/IEC TS 27100:2020将网络空间定义为一个由网络、服务、系统、人员、进程、组织以及存在于数字环境或通过其传输的要素所构成的相互连接的数字环境<sup>[5]</sup>。由此可见，网络是网络空间的子集。

随着网络边界不断延展，网络空间暴露面急剧增大，信任威胁日益多样化和复杂化，传统网络信任体系定义中的功能框架难以涵盖当前网络空间信任体系所需的全部核心能力。因此亟需探索身份认证、授权管理和责任认定传统三大核心特征之外的网络空间信任体系的新增特征，并系统分析其在典型应用领域中面临的风险挑战。

当前，关于网络空间信任体系的研究主要聚焦于宏观政策层面或具体信任模型的应用探索。例

如，有学者根据数字信任体系构建需求，提出一种面向国家数字信任体系的建设框架<sup>[6]</sup>；也有研究聚焦零信任等典型信任模型在不同网络环境中的应用，针对其应用效果提出发展路径和优化建议<sup>[7-9]</sup>；还有部分研究从网络信任体系发展趋势角度，探讨了信任体系的未来演进方向<sup>[10,11]</sup>。尽管上述研究具有较强的战略意义和理论价值，但当前仍缺乏对网络空间信任体系核心功能特征的研究。同时，现有信任模型大多面向特定场景或基于特定基础模型构建，缺少一种从网络空间安全技术视角出发的网络空间信任体系，难以支撑对不同场景下的网络空间信任体系的核心技术和信任风险进行系统分析。

本文在梳理网络空间信任体系发展态势的基础上，深入分析网络空间信任体系需求，提出技术视角下的网络空间信任体系模型，并探讨未来网络空间信任体系的核心特征和典型应用中的信任问题。最后，研究提出相应的风险应对策略，为保障网络空间的安全稳定，推动数字经济健康发展，维护国家利益和社会秩序提供理论支撑。

### 二、世界主要国家信任体系发展过程与趋势

#### （一）美国网络空间信任体系发展过程

美国网络空间信任体系经历了近30年的发展，实现了从单一化认证功能到体系化信任建设的过程，与信任相关的政策最早可追溯到1995年美国犹他州出台的《数字签名法》<sup>[12]</sup>，为后续世界各国电子签名立法提供了重要范本。为应对日益严重的身份伪造和中间人攻击问题，统一跨州及国际商务信任基础，美国于2011年4月发布了《网络空间可信身份国家战略》<sup>[13]</sup>，该政策旨在解决网络身份信任缺失问题，计划用10年时间构建覆盖全国的身份生态系统。随着云计算技术的发展，其多租户、动态资源分配和分布式架构等特征带来新的安全威胁，传统基于网络边界的虚拟专用网络（VPN）架构无法满足其安全可信需求，同时安全威胁暴露面持续扩大，因此美国政府和产业界加速推进零信任架构研究与落地。2020年，美国国家标准与技术研究院发布了第一个零信任技术标准“Zero Trust Architecture”

(SP 800-207, ZTA), 该标准成为全球首部由权威研究机构发布的零信任架构官方参考文件<sup>[14]</sup>。ZTA明确提出零信任的七大原则, 并定义了逻辑组件, 构建了具备可落地实施的技术架构体系。

2020年, SolarWinds 供应链攻击等事件暴露了传统“城堡与护城河”模型的脆弱性, 同时一些因素影响推高了线上办公比例。在此背景下, 2021年5月, 时任美国总统拜登签署了第14028号行政命令《改善国家网络安全》(Executive Order 14028)<sup>[15]</sup>, 要求联邦机构在2024财年结束前完成零信任架构(ZTA)的部署。此举标志着零信任理念成为美国网络空间安全的核心战略方向之一, 也标志着美国网络安全战略从传统边界防御向动态信任验证的范式转变。为落实Executive Order 14028行政令的要求, 美国网络安全与基础设施安全局(CISA)发布了零信任成熟度模型(ZTMM)1.0<sup>[16]</sup>, 作为美国联邦机构实施零信任架构的核心指导框架, 强调从传统边界防御向零信任的过渡<sup>[17]</sup>。2023年4月, CISA发布了ZTMM 2.0版本(2024年进一步修订), 进一步细化了成熟度阶段、增强技术指导<sup>[18]</sup>。新版本进一步适应混合办公、云原生环境等新应用场景, 强化了动态风险适应的能力, 体现了网络空间信任体系架构需根据实际需求和应用场景持续演进的技术特征。此外, 2022年美国国防部(DoD)提出《零信任战略》, 标志着美军网络安全体系从传统边界防御向动态验证、以数据为中心的安全模式全面转型<sup>[19]</sup>。

## (二) 我国网络空间信任体系发展过程

我国网络空间信任体系起源于对身份伪造的防范, 并随着可信需求的变化逐步发展为多功能协同的复杂体系, 在此期间政策和技术双轮驱动, 推动信任体系持续演进。从政策角度看, 2004年8月审议通过了《中华人民共和国电子签名法》, 并在2015年4月和2019年4月进行了两次修订; 该法明确了电子签名的定义、格式、适用范围和法律效力, 有力地支撑了网络信任体系建设。2006年2月, 国家网络与信息安全协调小组发布了《关于网络信任体系建设的若干意见》<sup>[3]</sup>, 明确定义了网络信任体系是以密码技术为基础的完整体系, 并提出了建设目标和指导原则。2006年《国家中长期科学和技术发展规划纲要(2006—2020年)》(国发

(2005) 44号) 也将网络信任体系列为信息安全领域的优先主题, 标志着其建设被提升至国家科技发展战略高度。2017年6月, 《中华人民共和国网络安全法》正式施行, 其中第二十四条明确提出国家实施网络可信身份战略, 支持安全、方便的电子身份认证技术, 推动不同认证体系间的互认, 为网络信任体系的深化发展提供了依据。2021年《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》发布, 与《中华人民共和国网络安全法》一起作为维护数据可信、隐私保护的法律法规。2024年7月, 公安部、国家互联网信息办公室发布了《国家网络身份认证公共服务管理办法(征求意见稿)》, 旨在推进国家网络可信身份战略, 强化公民个人信息保护, 并规范网络身份认证公共服务建设应用。

从技术标准框架角度看, “十四五”规划及工业和信息化部发布的《网络安全产业高质量发展三年行动计划(2021—2023年)》等政策文件将可信计算列为重点发展对象。相关技术标准包括《信息安全技术 可信计算规范 可信软件基》(GB/T 37935—2019)<sup>[20]</sup>、《信息安全技术 可信计算 可信计算体系结构》(GB/T 38638—2020)<sup>[21]</sup>、《信息安全技术 可信计算 可信连接测试方法》(GB/T 38644—2020)<sup>[22]</sup>等, 旨在从计算平台的底层构建信任根, 实现对系统行为的度量和控制, 为网络信任提供内生安全支持。同时我国也在积极探索零信任体系的未来发展方向。2024年《网络安全技术 零信任参考体系架构》(GB/T 43696—2024)发布, 为各行业落实零信任提供了权威的技术框架和指导<sup>[23]</sup>。

## (三) 其他世界主要国家网络空间信任体系发展过程

欧盟高度重视网络空间信任建设, 2018年发布了《通用数据保护条例》(GDPR), 推动隐私保护、数据安全的相关措施落实落地, 为信任建设提供了坚实的法律基础<sup>[24]</sup>; 2024年欧盟发布了《欧盟网络安全认证框架》(EUCC), 该框架涵盖了一系列规则、技术要求、标准和程序, 旨在通过建立统一的、高标准的认证框架来消除成员国间的数字壁垒, 增强内部单一市场的互信, 并向全球输出其基于规则和价值观的治理模式<sup>[25]</sup>。日本于2001年实施《电子签名和认证业务法》, 赋予电子签名法律效力,

建立远程签名服务商认证标准；2025年3月正式发布了《日本网络安全技术评估要求》(JC-STAR)，旨在通过清晰的定量评估标准和结果，提高物联网产品网络安全措施的透明度，从而增强消费者的信任<sup>[26]</sup>。

2018年，巴西政府发布了《通用数据保护法》，旨在从法律角度保护公民隐私，促进数据安全性<sup>[27]</sup>。2018年，加拿大推行《个人信息保护和电子文件法》，敦促企业推出切实有效的方法以保护消费者隐私权益<sup>[27]</sup>；2023年加拿大政府发布了《加拿大全国信任框架》(PCTF)，通过身份认证、数字钱包、隐私保护、凭证管理等功能模块，维护数字身份生态系统的互操作性与可信度<sup>[28]</sup>。

#### (四) 未来网络空间信任体系发展趋势分析

随着网络空间的不断扩张，网络空间的技术应用场景逐渐增多。应用场景的演进会引发网络空间信任需求的变化，进而推动网络空间信任体系技术与架构发生变化。21世纪初，网络信任体系的核心功能为保障身份认证的唯一性和不可抵赖性，随着数据的重要性不断提升，网络信任体系的核心功能逐渐向数据安全保护和隐私保护倾斜。同时随着云计算、分布式计算等技术的不断发展，网络空间的暴露面逐渐增多，零信任等新技术架构随之诞生，网络空间扩展带来的信任风险是驱动信任体系演进的重要原因。因此需要基于网络信任体系的应用场景和面临风险探索未来网络空间信任体系需具备的功能特征。

目前已有的信任体系模型框架可以分为两类，一是针对网络空间可信建设而提出的防御模型，包括美国发布的SP 800-207、《零信任战略》，我国发布的可信计算、零信任体系相关政策标准，欧盟发布的GDPR、EUCC等条例和框架，旨在维护可信网络空间，保障实体之间身份认证的可信性，同时保护数据和隐私的安全性。二是针对网络空间可信产品的评价模型，包括美国发布的ZTMM成熟度模型、日本发布的JC-STAR模型等，多用于评估产品的可信度和成熟度，为产品的落地应用提供参考。然而，在新技术不断涌现的背景下，不仅需要已有产品进行可信度评价，还需要对新技术、新应用的可信风险进行评估和预测。针对该需求，可以从技术视角出发提出信任体系分析框架，支撑对

信任技术及其功能应用的风险识别与分析。

### 三、基于技术视角的网络空间信任体系模型

#### (一) 网络空间信任体系基础框架构建

网络空间技术体系分为通信层技术、网络层技术、系统层技术、应用层技术等4个层次，如图1所示。其中，应用层进一步细分为通用应用层和领域应用层<sup>[29]</sup>，每一技术层均面临相应的信任问题，并产生针对性的信任技术。因此，本研究从网络空间技术体系角度出发，提出了网络空间信任体系基础框架，包含5个技术层：分别为通信信任技术层、网络连接信任技术层、计算系统信任技术层、通用应用信任技术层、领域应用信任技术层，如图1所示。该框架能够系统地识别关键技术要素，进而系统构建面向技术要素的网络空间信任体系。

为梳理技术视角下网络空间信任体系的内涵，分析各层中信任技术的构成，本研究从横向视角研究网络空间中每一技术层面临的信任问题，如图2所示，系统梳理相应的信任技术，为后续技术风险评估提供支撑。

##### 1. 通信层信任问题及对应技术

通信层关注点对点数据传输，其信任问题可归纳为三类：身份不可信、信号不可信、链路不可信。其中，身份不可信问题多由局域网地址(MAC)伪造、地址解析协议(ARP)欺骗等中间人攻击引发，可能导致通信节点身份伪造、密钥泄露等安全风险。应对技术包括物理不可克隆函数(PUF)、射频指纹识别、量子密钥分发、MACsec、WPA3协议、802.1X认证、动态ARP检测等，主要用于

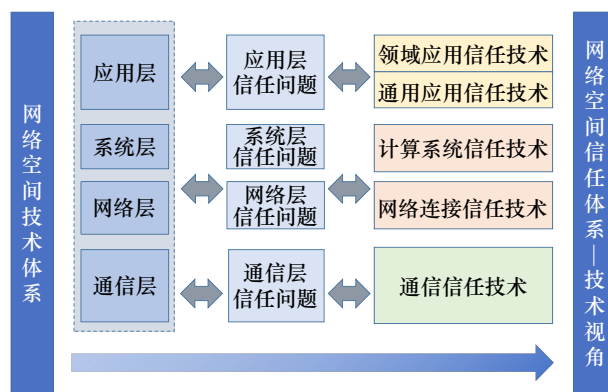


图1 基于网络空间技术要素构建网络空间信任体系的逻辑原理

解决硬件级的身份认证和密钥安全防护。信号不可信表现为干扰攻击、信号失真、数据丢失，影响数据包的完整性和可达性。对应的解决技术包括跳频扩频、纠错技术、重传机制等，提升保障信号传输的可靠性；同时，结合时钟同步优化、流量整形、冲突避免与退避算法等技术可进一步提升传输性能。链路不可信主要源于功耗分析、侧信道攻击、物理窃听，可能导致数据包在传输过程中面临被物理监听等风险。应对的技术有位置关联信号处理、人工噪声注入等技术，增强链路的抗监听能力。

## 2. 网络层信任问题及对应技术

网络层的信任问题主要归纳为路由（路径）不可信、地址不可信、域名不可信3个方面。其中，路由不可信主要源于路径篡改、流量篡改和通信监听等攻击行为，可能导致数据包被重定向、篡改或泄露。应对技术包括BGPsec、可信路由机制以及IPsec等，用于增强路径验证与数据传输加密能力。地址不可信问题多由IP地址伪造所引发，典型如反射放大攻击等。解决该类问题的信任技术包括真实源地址验证（SAVA）和资源公钥基础设施（RPKI），前者保障源地址的真实性，后者用于验证IP地址与自治系统之间的绑定关系。域名不可信通常源于域名系统（DNS）劫持、缓存投毒等攻击，可能导致用户访问被重定向至恶意站点。对应的防护技术包括域名系统安全扩展（DNSsec）和安全套接层/传输层安全性（SSL/TLS）协议，用于保障域名解析过程的完整性与可信性。

## 3. 计算系统层信任问题及对应技术

计算系统层主要关注计算终端的核心组件，如

中央处理器、芯片、操作系统等。该层的信任问题可以分为：硬件不可信、操作系统不可信、进程不可信3个方面。其中，硬件不可信问题源于供应链污染（如硬件木马、芯片后门）和侧信道攻击等，可能会导致硬件漏洞被恶意利用，造成信息泄露甚至引发信任链崩塌等严重后果。解决方案包括硬件信任根、形式化验证、人工噪声注入等技术，用以验证硬件的安全性和完整性。操作系统不可信涵盖了内核安全与固件安全问题（固件漏洞、固件篡改）等，可能导致固件持久化控制和内核权限劫持等风险。解决方案包括最小化可信计算基（如微内核架构、形式化验证等）、安全启动机制（如固件校验）以及资源隔离技术等，确保固件和内核的安全性。进程不可信表现为数据泄露、隐私侵犯、恶意提权攻击等，该问题将导致数据流动的不安全性，造成数据泄露隐私安全问题。应对技术包括可信执行环境、动态度量机制等，通过运行时评估与隔离手段校验进程级操作的可信度和可控性。

## 4. 通用应用层信任问题及对应技术

通用应用层的信任问题主要包括：身份不可信、服务不可信、数据不可信、软件不可信4个方面。其中，身份不可信通常由身份伪造、弱认证机制、权限分配不当等引发，可能导致未授权访问及应用的恶意提权风险。现有应对技术包括多因素认证技术（MFA）、无密码认证技术（FIDO）、基于属性的细粒度访问控制、零信任架构、公钥基础设施（PKI）等。服务不可信主要源于CA不可信、域名服务不可信等，该不可信问题不仅存在技术挑战，还涉及国际话语权争夺与证书体系建设等网络

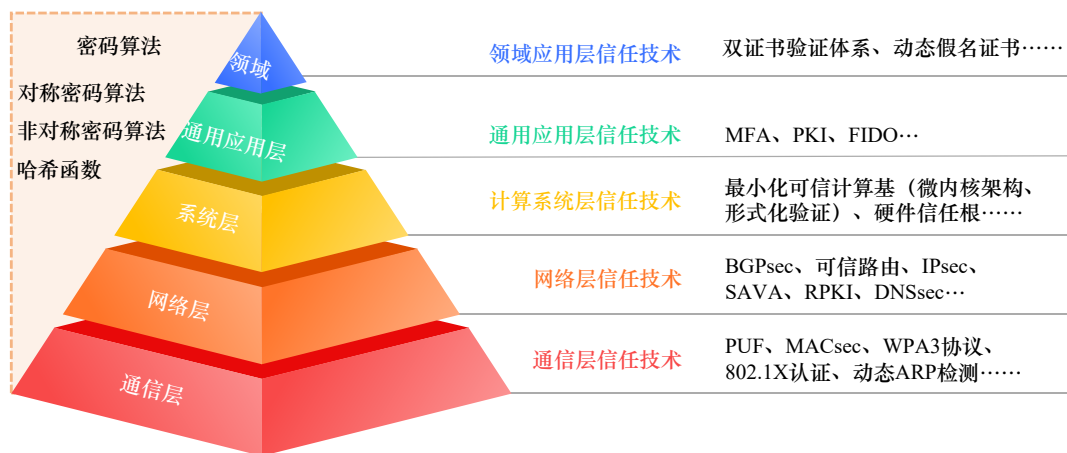


图2 基于技术视角的网络空间信任体系框架

空间治理能力。数据不可信表现在数据泄露、篡改、侧信道攻击、会话劫持、非法注入等，对应的解决方案包括端到端加密技术、隐私保护技术（差分隐私）、完整性验证机制（数字签名、哈希校验、区块链技术）等。软件不可信主要指软件供应链污染（如植入恶意代码）、软件漏洞利用等，常用的防护技术包括数字签名、软件供应链治理等。

领域应用层主要关注包括医疗、金融、车联网在内的特殊场景的可信需求和特有可信技术。例如，医疗领域更加强调患者数据隐私与系统互操作性；金融场景则侧重可信身份认证与交易不可抵赖性；车联网则聚焦于轻量级证书机制实现快速身份认证与数据完整性保护的平衡。本文在后续第四章将对四种典型应用进行风险及技术分析，丰富领域应用可信需求与技术的内容。

由于加密算法是网络空间信任体系的基础，因此本文将包含对称密码算法、非对称密码算法，以及哈希函数在内的密码学基础纳入网络空间信任体系模型框架中，该框架从技术视角出发有效地支撑对信任技术及其功能应用的风险识别与分析。

### （二）网络空间信任体系核心功能特征

随着网络空间不断扩张，网络空间信任体系的核心功能特征也随着发生变化。本节将从纵向角度对信任体系框架开展分析，重点探讨各技术层之间的功能关联与共性特征，进而凝练出网络空间信任体系的关键功能要素。

#### 1. 身份认证、授权管理、责任认定

我国在《关于网络信任体系建设若干意见的通知》中明确提出了，网络信任体系的核心功能特征包括身份认证、授权管理、责任认定3个方面<sup>[3]</sup>。网络是网络空间的重要组成部分，网络空间信任体系理论上也应包含这三项核心功能。从技术层面分析，网络空间信任体系各技术层均体现出上述三项特征的技术支撑。例如，通信层中MACsec、动态ARP检测等技术可有效解决MAC地址伪造、ARP欺骗等问题，实现底层身份认证；网络层中利用SAVA、RPKI等技术，可实现IP源地址的真实性核验以及边界网关协议（BGP）路由通告的合法性，以解决网络层身份认证问题；计算系统层面对恶意提权攻击等授权管理问题，可用动态度量等技术加强系统可信执行保障；应用层中则广泛应用PKI、

FIDO等技术实现访问控制与身份认证。因此，网络空间信任体系在技术实现上具备了身份认证、授权管理、责任认定三项功能特征。

此外，信任体系的功能实现需要不同技术层之间的协同配合。以身份认证功能为例，在公用互联网复杂环境下，实体间的身份认证往往需要不同技术层之间的协同支撑。具体而言，通信层可通过MACsec技术保障MAC地址的可信性，网络层则利用SAVA、RPKI等技术，确保数据面和控制面的地址可信性。在通信层和网络层身份认证的基础上，应用层通常使用PKI技术验证实体的身份有效性。由此可见，在特定场景下，围绕身份认证的信任需求，需自下向上逐层构建信任技术，建立跨层协同的信任体系。

#### 2. 数据可信

截至2024年，全球数据总量已突破180 ZB，其中我国年度数据生产总量达41.06 ZB，占全球总量的23%，同比增长25%。与此同时，针对数据窃取等行为的网络攻击事件频发，数据安全威胁日益严峻。数据可信是指数据在其全生命周期中保持真实性、完整性、可用性等核心特性，并通过技术与管理手段保障其来源可靠、处理合规、结果可验证及机密性。随着人工智能、大数据的新应用不断涌现，围绕训练数据、输出结果的可信性评价以及隐私保护等方面的信任需求迅速增长，数据可信已成为网络空间信任体系中的重要特征之一。

从技术视角来看，如图3所示，网络空间信任体系在不同层级均面临数据安全威胁，具体而言，通信层存在物理窃听问题，网络层面面临流量监听、流量篡改问题，系统层可能存在数据泄露、隐私侵犯等问题，应用层则存在数据泄露篡改、非法注入、侧信道攻击等问题。针对这些问题，相应的信任技术包括跳频扩频、人工噪声注入、哈希函数、透明数据加密、差分隐私等多种技术，用于保障数据传输与处理的安全性和完整性。因此，网络空间信任体系应具备维护数据可信的功能特性。

#### 3. 供应链与服务可信

2020年11月，“太阳风暴”攻击事件导致全球多个国家和地区超过18 000个用户的数据泄露，直接经济损失达数十亿美元<sup>[30]</sup>。2024年9月，黎巴嫩多地发生手持寻呼机爆炸事件，造成12人死亡<sup>[31]</sup>。这些事件表明，保障供应链和服务安全可信发展



图3 网络空间信任体系核心功能特征分析

注：TDE为透明数据加密。

成为网络空间最为迫切的可信需求之一，对国家关键信息基础设施的安全保障具有重要的战略意义。

从技术层面看，系统层、网络层、应用层均存在不同形式的供应链安全风险。例如，系统层面临内核和固件安全风险，如固件后门；网络层存在DNS服务不可信风险；应用层则面临软件供应链不可信及认证机构不可信问题。针对上述问题，相应的信任技术包括硬件信任根、形式化验证、数字签名、供应链治理等。

如图3所示，身份认证、授权管理、责任认定、数据可信、供应链与服务可信等5项功能从技术层面覆盖了网络空间信任的关键要素，为构建系统化、可实现、可验证的网络空间信任体系提供了理论支撑。

#### 四、网络空间信任体系典型场景应用分析

当前公用互联网信任关系主要依赖PKI体系建立，其信任锚是根证书颁发机构（Root CA）的公钥证书，是整个信任体系的绝对信任起点<sup>[32]</sup>。PKI体系通过一种基于层级数字签名验证的信任传递机制构建信任链，即通过信任锚点逐级向下签发数字证书，形成可追溯的信任路径。这种中心化树状结构不仅实现了信任的委托和规模化扩展，还通过严格的证书策略，如证书吊销列表（CRL）、在线证书状态协议（OCSP），确保信任链的动态安全

性<sup>[33]</sup>。然而，在某些具有特殊需求的应用场景中，PKI体系存在适用性不足的问题，难以建立满足需求的网络空间信任体系。为此，基于前文提出的技术视角下的网络空间信任体系框架，按照高战略性、高关注度、技术发展代表性的原则，选取4种典型场景进行分析，如图4所示，探讨其信任体系构建方式、面临的信任风险和可用信任技术，为后续网络空间信任体系发展的策略提供理论支撑。

##### （一）极端条件下网络空间信任风险与技术

在极端条件下，现有网络空间信任体系存在失效风险，因此亟需重点研究其在极端环境中的信任风险与解决技术。此类场景的主要风险集中于网络空间技术体系中的网络层和通信层，并在一定程度上延伸至应用层。在通信层，物理链路如光缆、天线等可能被人为破坏或自然灾害而中断，导致信号无法传输，使通信载体无法承担身份认证或信任建立作用。在网络层，路由链路可能被限制或阻断特定IP的数据传输，还可能面临路由挟持等威胁，导致路由不可信。在应用层，由于现有PKI体系采用中心化信任链验证机制，在极端条件下存在单点失效的问题，例如中间CA证书被根CA吊销，导致由中间CA签发的终端证书失效，影响大量PKI的认证服务。此外，DNS解析服务也可能遭受大规模拒绝服务的威胁，导致域名解析失败，进而导致大量用户无法访问关键服务。

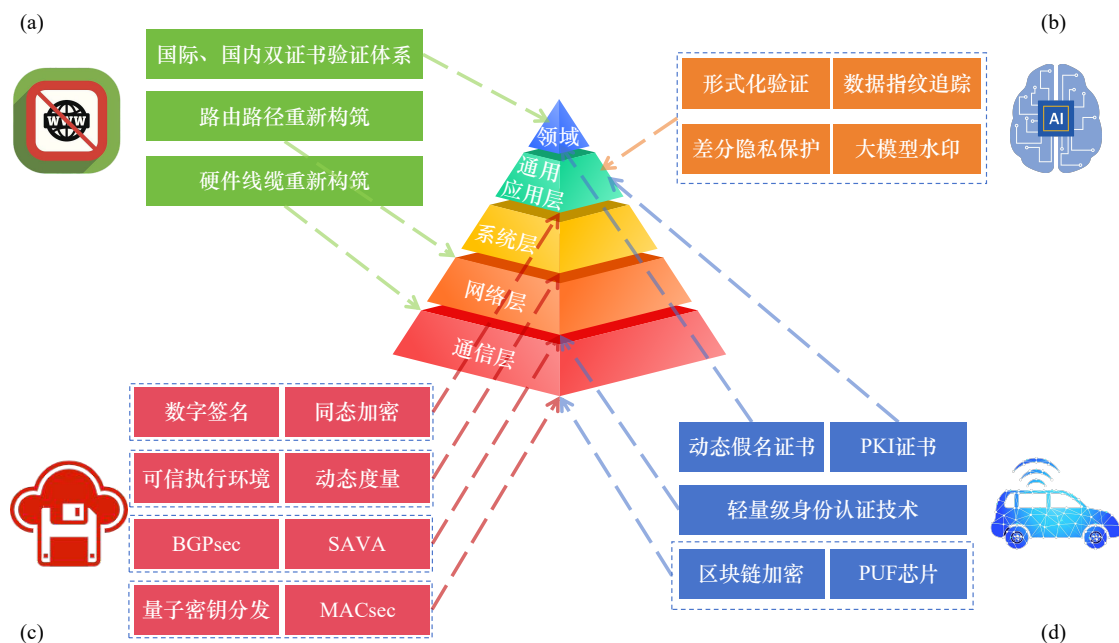


图4 基于技术视角的网络空间信任体系模型在典型场景下的信任风险及技术分析

注：(a) 以极端条件下网络空间场景为例；(b) 以人工智能大模型场景为例；(c) 以数据流通场景为例；(d) 以车联网场景为例。

针对上述信任威胁，在极端条件下可采用相应的信任技术解决上述信任问题，如图4（a）所示，通信层可以采用快速部署备用硬件链路方式重构通信通道，网络层可以采用定制化扩展 RPKI 的方式确保网络层控制面可信，同时可以隐蔽路由、域名伪装的方式，结合域外的路由节点或者改变报文 IP 地址的方式绕过对我方的 IP 地址限制，应用层则需要推动国际、国内双证书体系建设，探究去中心化的身份认证机制。

## （二）大模型时代信任风险与技术

随着大模型技术的飞速发展，基于大模型的各类问题层出不穷，在构建其信任架构的过程中，除关注通信层、网络层、系统层的基础信任保障外，其面临的信任风险和关键技术多集中于通用应用层。该场景下的信任需求体现在模型可信、训练数据可信、输出结果可信 3 个方面<sup>[34]</sup>。

在模型可信方面，当前人工智能大模型普遍存在“黑箱”特征，缺乏足够的可解释性，决策逻辑过程难以追溯，天然带有不可信的属性。同时，模型易受到对抗性攻击和恶意篡改，进一步加剧了模型的不可控性与不可解释性。在训练数据可信方面，攻击者可通过在正常训练样本中置入攻击数据，导致模型识别精度下降、理解出现偏差、进而

引发分类错误、输出结果非预期甚至相悖。此外，随着大模型参数规模不断扩大，预训练数据呈指数级增长，若攻击者利用特定方法对训练数据进行信息推理或重构，可能会从中提取到用户的敏感信息，造成数据隐私泄露。在输出结果可信方面，人工智能生成内容的信任风险可分为大模型“幻觉”和生成内容滥用。大模型的“幻觉”现象会生成虚构信息或无法验证的信息，严重影响结果的可靠性与可用性，同时生成内容滥用会导致虚假新闻泛滥，产生伦理问题甚至影响国家发展。此外，人工智能的输出结果还可能用于恶意诽谤、学术不端等行为，严重侵害他人合法权益、影响社会秩序。

针对生成式人工智能的信任需求，如图4（b）所示，目前可以通过形式化验证、可解释性工具增加模型的可信度；通过差分隐私保护、数据指纹追踪确保训练集的数据可信；通过动态监控机制、深伪检测工具检测保障输出数据可信。目前大模型水印技术常用于深伪检测等领域，是一种为人工智能生成内容（如文本、图像、代码等）嵌入隐蔽但可检测的“标记”技术，其目的是识别和溯源，确保内容安全可信。通过上述多层次的信任技术协同保障，可有效应对生成式人工智能在可信性方面面临的挑战。

### （三）数据流通下的可信风险与技术

根据国家数据局发布的《可信数据空间发展行动计划（2024—2028年）》中对可信数据空间的定义，可信数据空间是基于共识规则，联接多方主体，实现数据资源共享共用的一种数据流通利用基础设施，是数据要素价值共创的应用生态，是支撑构建全国一体化数据市场的重要载体。因此该场景需重点关注数据资源保护和资源共享中的可信需求。在通信层，数据在物理链路上流动时面临物理窃听、信号干扰与链路劫持等风险，导致数据在硬件传输时被泄露或篡改。数据包在网络层的传输路径面临路由劫持、地址欺骗等威胁，可能导致数据被重定向至恶意节点。在系统层与通用应用层，数据在计算节点处理与暂存时面临因硬件漏洞、恶意软件或未授权进程导致的数据泄露与篡改风险。

基于以上可信风险分析，各层的可信技术如下：通信层的可信技术包括量子密钥分发与MACsec等，保障数据在该技术层的机密性与完整性；网络层的可信技术包括BGPsec与SAVA技术等，维护数据传输路径与来源的可信；系统层的可信技术包括可信执行环境、动态度量等，为关键计算提供隔离且可验证的信任根；在应用层数据本身的可信保障上，密码学哈希函数与数字签名技术为数据完整性验证提供了核心支撑，而差分隐私、同态加密等隐私增强技术则能在数据使用与流通环节实现数据有效利用与隐私保护需求的平衡。

### （四）车联网场景下的信任风险与技术

随着物联网、工业互联网等新技术应用的不断发展，信任风险与应对技术不仅体现在通用应用层及以下技术层，在领域应用层同样呈现出独特的信任需求和技术特性。本节以车联网场景为例，系统分析其面临的信任风险，并探讨对应的信任技术。

在车联网应用场景中，传统的PKI体系证书系统难以完全满足其多样化与高实时性的信任需求。具体挑战体现在：在网络传输层，车联网中通信系统要求能够对紧急事件做出毫秒级响应，而传统PKI中链式证书验证需要多级CA回溯进行身份确权，难以满足车载高速移动环境下的超低时延认证需求<sup>[35]</sup>；在系统层，车载单元等计算系统资源受限，而传统证书体积较大（约1~4 kB），在资源受限的硬件平台上运行将造成额外开销，严重影响关

键功能的实时性和可靠性<sup>[36]</sup>；在应用层，传统PKI体系中由根CA和中间CA颁发的证书通常有较长的有效期，攻击者可利用固定证书中的标识信息进行车辆跟踪与定位，严重威胁用户隐私安全。因此，在车联网场景下，直接应用传统PKI信任体系存在明显局限性，需结合场景特性对信任机制进行适配与优化<sup>[37,38]</sup>。

基于车联网应用场景中信任体系构建的特定需求，应在各技术层采用不同的可信技术方案，如图4（c）所示。在网络层，为满足快速身份认证功能的要求，可采用区块链加密、PUF芯片结合椭圆曲线证书、轻量级证书等方式，实现低延迟、高可靠的快速身份确权和认证响应。在应用层，针对数据可信与隐私保护需求，可采用假名CA签发临时证书或动态假名证书方式。此类假名证书不包含车辆识别码、车主信息等敏感数据，仅包括加密的公钥和短时有效期信息，并以高频率动态更新，从而有效降低数据的持续泄露风险，增强车联网场景下的数据可信能力。

## 五、我国网络空间信任体系发展建议

本文系统梳理了世界主要国家网络空间信任体系的发展脉络，分析信任体系变迁背后的关键影响因素和未来发展需求。针对发展需求，本文提出了一种基于技术视角的网络空间信任体系模型框架，以网络空间各技术层为基础，突出技术要素与风险之间的关联，具备良好的风险分析能力与架构扩展性，可适应未来网络空间信任体系的演化趋势与新风险环境变化。本文分析了网络空间信任体系的核心功能特性：身份认证、授权管理、责任认定、数据可信以及供应链与服务可信等；为验证模型的适用性，选取了极端网络空间场景、人工智能大模型场景、数据流通场景、车联网场景4个网络空间典型应用场景，深入分析面临的信任风险与应对技术，进一步体现了该框架在实际应用中的可操作性。

综上所述，本研究为我国网络空间信任体系建设和演进提供了技术支撑和理论参考。建议从以下几方面开展后续工作。

### （一）推动可信基础设施建设，筑牢信任基石

为提升我国网络空间信任体系网络层的可信能

力，建议积极推动 SAVA、RPKI 等新兴关键技术落地与应用，从数据面与控制面两个维度系统解决源地址真实性与路由可信安全问题。从数据面角度，可以专用网络环境为切入点，开展 SAVA 部署试点，在国际网关探索“电子护照”机制，通过源地址溯源认证增强源地址真实性保障能力，以渐进式开放路径逐步向大规模网络环境推广。从控制面角度，大力推动基于 RPKI 的路由起源授权（ROA）及其验证机制（ROV）的部署与应用，扩大其覆盖范围，并强化 RPKI 信任锚证书的动态校验机制，以降低因证书配置错误或失效引发的路由安全事件风险。此外，在技术标准层面，建议推动跨国 RPKI 验证联盟，统一信任锚配置与验证机制，完善相关国际标准，将 RPKI 升级为支撑全球可信路由的基座型基础设施。

### （二）采取多层次信任策略，逐层解决网络空间信任问题

为更高效地解决网络空间多样化信任需求，在技术视角下的信任体系框架中，明确通信层、网络层、系统层、应用层等各技术层的责任主体与实施路径。通信层、网络层主要由网络基础设施运营商承担保障信任责任，确保传输链路的安全加密、网络节点的可信接入以及网络服务的高可用性。系统层依赖于设备制造商与系统集成商，其核心任务包括实施硬件可信根、固件安全启动、操作系统层面的安全增强与可信度量。应用层则由应用开发商和服务提供商承担，着重构建用户身份强认证、数据隐私保护、交易不可抵赖性以及抵御应用层面的攻击等。与试图构建一个庞大而统一的“全局信任”模型相比，采用分层责任划分与逐层技术应对的模式，在应对不同层级信任威胁方面具有更高的执行效率、策略针对性、体系韧性，是系统构建可扩展网络空间信任体系的现实路径。

### （三）加强信任体系韧性建设，探究去中心化信任构建方式

当前 PKI 体系中的信任锚高度依赖于少数根证书颁发机构，这一中心化信任架构在提供信任基础的同时，也存在诸多结构性风险。例如，单点失效风险高、根密钥或重要中间 CA 密钥泄露危害大等问题。为提升网络空间信任体系的弹性与抗风险能

力，亟需探索去中心化证书体系的新路径。例如，可借助区块链、分布式账本技术构建去中心化的证书透明签发、验证与撤销机制，避免对传统根 CA 的单点依赖。通过引入密码学共识机制，实现证书操作的开放性、透明性与抗篡改性等，从根本上提升网络空间信任体系的透明度与韧性。

### （四）重点关注软硬件供应链可信建设，打造自主可控的支撑体系

鉴于近年来针对软硬件供应链的攻击事件日益频繁且危害范围广、影响大，基础设施的自主可控能力提升已成为国家战略支点。为有效应对供应链信任风险，应加快推进软硬件供应链国产化替代与可信保障能力建设。在供应链的自主可控研发方面，以硬件设备、操作系统、工业软件等基础层技术突破为驱动，强化基础性投入与体系化创新，推动信创国产化替代产品落地应用，从被动应急转向主动布局的战略转变。在供应链可信保障方面，需加强可信计算、可信度量等关键技术研究，推动构建覆盖上下游产业链的软硬件安全测试与评估平台，实现对元器件、操作系统、固件、应用软件等环节系统性验证与风险识别，整体提升供应链安全韧性。

### （五）重点关注极端条件下网络空间信任体系重构问题

在极端对抗场景下，传统信任体系可能面临多层次瓦解风险，对基础服务的持续可用性与信任链条的完整性构成巨大挑战。在通信层，可能面临海缆中断、卫星链路干扰等物理层破坏，导致链路不可用。在网络层，存在路由劫持、路由重定向等风险，破坏数据传输的可信性。在应用层，可能遭遇境外证书吊销、DNS 污染与屏蔽等威胁，导致身份认证失败与关键服务不可访问等。针对上述风险，应高度关注极端环境条件下网络空间的可信保障问题，积极加强利用隐蔽路由、域名伪装等隐蔽通信与伪装技术，提升关键基础设施服务在受限环节下的生成与抗干扰能力，同时加快推进国家根证书与应急 DNS 平台部署与落地，提升在断网、封锁等极端条件下的身份认证连续性与服务可达性。

#### 利益冲突声明

本文作者在此声明不存在任何利益冲突或财务冲突。

**Received date:** August 18, 2025; **Revised date:** October 20, 2025

**Corresponding author:** Zhang Lei is an associate research fellow from Zhongguancun Laboratory. Her major research fields include network security, network optimization, etc. E-mail: zhanglei@zgclab.edu.cn

**Funding project:** Chinese Academy of Engineering project “Research on Risks of New Technologies and Applications in Cybersecurity” (2023-JB-13); Strategic Development Department of the China Association for Science and Technology project “Research on the Impact of New Technological Transformations on Cyberspace Security Situation and Countermeasures”

#### 参考文献

- [1] Syntyurenko O V, Gilyarevskii R S. Trends and risks of network technologies [J]. Scientific and Technical Information Processing, 2021, 48(2): 97–106.
- [2] Azevedo A C, Scheid E J, Franco M F, et al. Assessing SSL/TLS certificate centralization: Implications for digital sovereignty [EB/OL]. (2025-04-24)[2025-07-12]. <https://arxiv.org/abs/2504.16897>.
- [3] 何良生. 密码是构建网络信任体系的基石 [J]. 中国信息安全, 2021 (5): 58–60.  
He L S. Password is the cornerstone of building a network trust system [J]. China Information Security, 2021 (5): 58–60.
- [4] International Electrotechnical Commission. Industrial communication networks – Fieldbus specifications – Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series: IEC 61158-1: 2023 [S]. Geneva: IEC, 2023.
- [5] ISO/IEC. Information technology — Cybersecurity — Overview and concepts: ISO/IEC TS 27100: 2020 [S]. Geneva: ISO/IEC, 2020.
- [6] 尹一桦, 帅军军. 数字信任体系研究 [J]. 信息安全与通信保密, 2023, 21(9): 96–105.  
Yin Y H, Shuai J J. Research on digital trust system [J]. Information Security and Communications Privacy, 2023, 21(9): 96–105.
- [7] 姜丽敏, 丁宇征, 李金戈, 等. 对零信任的网络安全防护体系的研究与分析 [J]. 网络安全技术与应用, 2024 (7): 1–2.  
Jiang L M, Ding Y Z, Li J G, et al. Research and analysis of network security protection system with zero trust [J]. Network Security Technology & Application, 2024 (7): 1–2.
- [8] 徐华林. 基于零信任安全体系的网络安全技术架构研究 [J]. 网络安全和信息化, 2025 (4): 34–36.  
Xu H L. Research on network security technology architecture based on zero trust security system [J]. Cybersecurity & Informationization, 2025 (4): 34–36.
- [9] 周吉, 房冬丽, 丁文超, 等. 基于零信任的网络信任体系安全性评估技术 [J]. 网络安全技术与应用, 2025 (6): 18–22.  
Zhou J, Fang D L, Ding W C, et al. Security evaluation technology of network trust system based on zero trust [J]. Network Security Technology & Application, 2025 (6): 18–22.
- [10] 严霄凤. 关于国家网络信任体系建设的思考 [J]. 信息安全与技术, 2011, 2(4): 3–4, 7.  
Yan X F. Thinking of constructing the national network trust system [J]. Information Security and Technology, 2011, 2(4): 3–4, 7.
- [11] 张立武. 网络信任体系发展趋势研究 [J]. 信息网络安全, 2011, 11(7): 69–71, 78.  
Zhang L W. Development trends of network trust system [J]. Netinfo Security, 2011, 11(7): 69–71, 78.
- [12] 陈远, 邱均平, 邹晶, 等. 对我国网络社区信息传播管理法规的思考 [J]. 山东社会科学, 2008 (5): 32–37.  
Chen Y, Qiu J P, Zou J, et al. Reflections on the management regulations of information dissemination in online communities in China [J]. Shandong Social Sciences, 2008 (5): 32–37.
- [13] Grant J A. The national strategy for trusted identities in cyberspace: Enhancing online choice, efficiency, security, and privacy through standards [J]. IEEE Internet Computing, 2011, 15(6): 80–84.
- [14] Rose W, Borchert O, Mitchell S, et al. Zero trust architecture [R]. Gaithersburg: National Institute of Standards and Technology, 2020.
- [15] 郝志超, 张依梦. 联邦零信任战略(译文) [J]. 信息安全与通信保密, 2022, 20(4): 44–51.  
Hao Z C, Zhang Y M. Federal zero trust strategy [J]. Information Security and Communications Privacy, 2022, 20(4): 44–51.
- [16] 许蔓舒. 以技术、政治和国际治理视角反思网络公开溯源 [J]. 中国信息安全, 2022 (5): 70–74.  
Xu M S. Reflection on the source of network openness from the perspective of technology, politics and international governance [J]. China Information Security, 2022 (5): 70–74.
- [17] 徐莉, 陈倩. 美国《国防部零信任参考架构》解读 [J]. 信息安全与通信保密, 2022, 20(1): 38–44.  
Xu L, Chen Q. Interpretation of U.S. DoD zero trust reference architecture [J]. Information Security and Communications Privacy, 2022, 20(1): 38–44.
- [18] 付国晴, 贾儒鹏, 吕玮. 2023 年网络安全热点技术领域全景扫描 [J]. 信息安全与通信保密, 2024, 22(1): 16–25.  
Fu G Q, Jia R P, Lyu W. Overview of cyber security technology hotspots in 2023 [J]. Information Security and Communications Privacy, 2024, 22(1): 16–25.
- [19] Department of Defense Office of Prepublication and Security Review. DoD zero trust strategy [R]. Washington, DC: Department of Defense, 2022.
- [20] 中国国家标准化管理委员会. 信息安全技术 可信计算规范 可信软件基: GB/T 37935—2019 [S]. 北京: 中国国家标准化管理委员会, 2019.  
National Standardization Administration Committee. Information security technology—Trusted computing specifications—Trusted software base: GB/T 37935—2019 [S]. Beijing: National Standardization Administration Committee, 2019.
- [21] 中国国家标准化管理委员会. GB/T 38638—2020 信息安全技术 可信计算 可信计算体系结构 [EB/OL]. (2020-04-28)[2025-07-12]. <https://openstd.samr.gov.cn/bz/gk/gb/newGbInfo?hcno=76B0E3C2D7898AF1DDB00E01C2DA88B0>.  
National Standardization Administration Committee. GB/T 38638—2020 Information security technology trusted computing trusted computing architecture [EB/OL]. (2020-04-28)[2025-07-12]. <https://openstd.samr.gov.cn/bz/gk/gb/newGbInfo?hcno=76B0E3C2D7898AF1DDB00E01C2DA88B0>.
- [22] 中国国家标准化管理委员会. GB/T 38644—2020 信息安全技术 可信计算 可信连接测试方法 [EB/OL]. (2020-04-28)[2025-07-12]. <https://openstd.samr.gov.cn/bz/gk/gb/newGbInfo?hcno=313886B1D7FDCD5FFAECAAA4C6417A52>.

- National Standardization Administration Committee. GB/T 38644—2020 Information security technology trusted computing trusted connection test methods [EB/OL]. (2020-04-28)[2025-07-12]. <https://openstd.samr.gov.cn/bz/gk/gb/newGbInfo?hcno=313886B1D7FDCD5FFAECAA4C6417A52>.
- [23] 国家标准化委员会. GB/T 43696—2024 网络安全技术 零信任参考体系架构 [EB/OL]. (2024-04-25)[2025-07-12]. <https://openstd.samr.gov.cn/bz/gk/std/newGbInfo?hcno=C166002FE253A840E56BEBF13B4945E7>.
- National Standardization Administration Committee. GB/T 43696—2024 network security technology zero trust reference architecture [EB/OL]. (2024-04-25)[2025-07-12]. <https://openstd.samr.gov.cn/bz/gk/std/newGbInfo?hcno=C166002FE253A840E56BEBF13B4945E7>.
- [24] 张宇光, 胡影. 2019年数据安全国际动态综述 [J]. 保密科学技术, 2019 (12): 32–35.
- Zhang Y G, Hu Y. Summary of international trends of data security in 2019 [J]. *Secrecy Science and Technology*, 2019 (12): 32–35.
- [25] European Commission. Implementing regulation on the adoption of a European Common Criteria-based cybersecurity certification scheme [EB/OL]. (2024-01-31)[2025-07-12]. <https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-adoption-european-common-criteria-based-cybersecurity-certification-scheme>.
- [26] Information-technology Promotion Agency. Japan cyber star (jc-star) [EB/OL]. (2024-09-30)[2025-07-12]. <https://www.ipa.go.jp/en/security/jc-star/index.html>.
- [27] Falowo O I, Popoola S, Riep J, et al. Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents [J]. *IEEE Access*, 2022, 10: 134038–134051.
- [28] 刘泽刚. 人工智能时代数字公民身份构建的要点、基点与难点 [J]. 法学评论, 2024, 42(5): 105–119.
- Liu Z G. Essence, basics and difficulties of constructing digital citizenship in the era of artificial intelligence [J]. *Law Review*, 2024, 42(5): 105–119.
- [29] 孙帅, 张蕾, 胡春卉, 等. 多视角下的网络空间安全模型与体系化发展 [J]. 中国工程科学, 2023, 25(6): 116–125.
- Sun S, Zhang L, Hu C H, et al. Cyberspace security models and systematic development from multiple perspectives [J]. *Strategic Study of CAE*, 2023, 25(6): 116–125.
- [30] Martínez J, Durán J M. Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study [J]. *International Journal of Safety and Security Engineering*, 2021, 11(5): 537–545.
- [31] 安雨康. 黎巴嫩寻呼机爆炸事件击穿全球供应链信任 [J]. 世界知识, 2024 (20): 48–50.
- An Y K. Lebanon pager explosion breaks trust in global supply chain [J]. *World Affairs*, 2024 (20): 48–50.
- [32] 徐恪, 凌思通, 李琦, 等. 基于区块链的网络安全体系结构与关键技术研究进展 [J]. 计算机学报, 2021, 44(1): 55–83.
- Xu K, Ling S T, Li Q, et al. Research progress of network security architecture and key technologies based on blockchain [J]. *Chinese Journal of Computers*, 2021, 44(1): 55–83.
- [33] 张宾, 张宇, 张伟哲, 等. PKI 技术与研究进展 [J]. 软件学报, 2025, 36(6): 2875–2899.
- Zhang B, Zhang Y, Zhang W Z, et al. Research and progress of PKI technology [J]. *Journal of Software*, 2025, 36(6): 2875–2899.
- [34] 刘晗, 李凯旋, 陈仪香. 人工智能系统可信性度量评估研究综述 [J]. 软件学报, 2023, 34(8): 3774–3792.
- Liu H, Li K X, Chen Y X. Survey on trustworthiness measurement for artificial intelligence systems [J]. *Journal of Software*, 2023, 34(8): 3774–3792.
- [35] 张海霞, 刘文杰, 薛彤, 等. 基于车辆行为分析的车联网超可靠低时延通信关键技术 [J]. 中兴通讯技术, 2020, 26(1): 12–18.
- Zhang H X, Liu W J, Xue T, et al. Vehicle behavior analysis based ultra-reliable and low-latency communication technologies for Internet of vehicles [J]. *ZTE Technology Journal*, 2020, 26(1): 12–18.
- [36] 章嘉彦, 李飞, 李如翔, 等. V2X 通信中基于椭圆曲线加密算法的身份认证研究 [J]. 汽车工程, 2020, 42(1): 27–32.
- Zhang J Y, Li F, Li R X, et al. Research on identity authentication in V2X communications based on elliptic curve encryption algorithm [J]. *Automotive Engineering*, 2020, 42(1): 27–32.
- [37] 刘召曼, 杨亚芳, 宁建廷, 等. 基于新型可净化多重签名的车联网高效假名证书分发方案 [J]. 通信学报, 2024, 45(11): 27–45.
- Liu Z M, Yang Y F, Ning J T, et al. Efficient pseudonym certificate distribution scheme for Internet of vehicles based on novel sanitizable multi-signature [J]. *Journal on Communications*, 2024, 45(11): 27–45.
- [38] 陆忠梅, 陈巍, 魏杰, 等. 车联网极低时延与高可靠通信: 现状与展望 [J]. 信号处理, 2019, 35(11): 1773–1783.
- Lu Z M, Chen W, Wei J, et al. Current situation and prospect of V2X with ultra-reliable and low-latency [J]. *Journal of Signal Processing*, 2019, 35(11): 1773–1783.