Advances in Applied Mathematics 应用数学进展, 2025, 14(6), 55-63
Published Online June 2025 in Hans. https://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2025.146300

Hans汉斯

云计算环境下网络安全关键技术研究现状与展望

——基于CiteSpace知识图谱的分析

张羽芳，王振龙，陈星源，蔡万林，陈海杏，庞正武*

广西民族大学数学科学学院，广西 南宁

收稿日期：2025年5月9日；录用日期：2025年6月2日；发布日期：2025年6月10日

摘　要

我国信息技术的跨越式发展催化云计算技术规模化应用，其通过资源虚拟化、弹性扩展和服务交付模式创新，推动传统集中式IT架构向分布式架构演进，实现软硬件资源解耦与服务化转型，成为驱动新基建和数字化转型的核心技术引擎。本文选取中国知网(CNKI)数据库以“云计算”和“网络安全”为主题检索筛选得到2057篇文献，并借助CiteSpace可视化分析软件绘制发文时间及发文量、关键词突现、关键词时区等知识图谱探究云计算环境下网络安全技术发展脉络；通过发文作者、关键词共现、关键词时间线等知识图谱对云计算环境下的网络安全关键技术的热点变更和趋势进行深入分析。结果表明，云计算网络安全攻防技术正进入常态化研究阶段，重点涵盖数据存储、网络、虚拟化和身份认证等领域。随着应用普及，数据泄露、账户安全和访问控制等风险凸显，推动网络安全技术朝着多元化、深度化和智能协同防御方向发展。因此，只有通过智能防御、加密技术、身份认证和多层防护等措施，才能构建安全可靠的云计算网络环境，促进网络安全关键技术的发展。

关键词

云计算，网络安全技术，CiteSpace

Research Status and Prospect of Network Security Key Technologies in Cloud Computing Environment

—Based on the Analysis of CiteSpace Knowledge Map

Yufang Zhang, Zhenlong Wang, Xingyuan Chen, Wanlin Cai, Haixing Chen, Zhengwu Pang*

*通讯作者。

文章引用: 张羽芳, 王振龙, 陈星源, 蔡万林, 陈海杏, 庞正武. 云计算环境下网络安全关键技术研究现状与展望[J]. 应用数学进展, 2025, 14(6): 55-63. DOI: 10.12677/aam.2025.146300

School of Mathematical Sciences, Guangxi Minzu University, Nanning Guangxi

Received: May 9th, 2025; accepted: Jun. 2nd, 2025; published: Jun. 10th, 2025

Abstract

The leapfrog development of information technology in China has catalyzed the large-scale application of cloud computing technology. Through resource virtualization, elastic scalability, and innovation in service delivery models, IT promotes the evolution of traditional centralized IT architectures to distributed architectures, achieving decoupling of software and hardware resources and service-oriented transformation, and has become the core technical engine driving new infrastructure and digital transformation. In this paper, 2057 papers were retrieved and screened from the China National Knowledge Infrastructure (CNKI) database with the themes of "cloud computing" and "cyber security", and knowledge graphs such as publication time and volume, keyword emergence, and keyword time zone were drawn with the help of CiteSpace visualization analysis software to explore the development context of cyber security technology in the cloud computing environment; the hotspots, changes and trends of key cyber security technologies in the cloud computing environment were analyzed through knowledge graphs such as authors, co-occurrence of keywords and keyword timelines. The results show that cloud computing network security attack and defense technologies are entering a regular research stage, with a focus on areas such as data storage, networking, virtualization, and identity authentication. With the widespread application, risks such as data leakage, account security and access control have become more prominent, driving the development of cyber security technology towards diversification, depth and intelligent collaborative defense. Therefore, only through measures such as intelligent defense, encryption technology, identity authentication and multi-layered protection can a secure and reliable cloud computing network environment be built to promote the development of key cyber security technologies.

Keywords

Cloud Computing, Network Security Technology, CiteSpace

1. 引言

1990 年，“网络安全”一词开始出现，此后不断有学者探讨网络环境下的安全问题。21 世纪全球步入数字文明纵深发展阶段，5G、AI 与产业互联网的深度融合驱动数字经济指数级增长；但攻击面扩张催生新型网络威胁产业化，据 Gartner 统计，2023 年全球 APT 攻击量同比激增 137%。在《网络安全法》与等保 2.0 框架下，我国正构建基于零信任的主动免疫体系，将网络空间安全提升至国家安全战略高度，护航关键信息基础设施安全稳定运行[1]。我国信息技术的快速发展促进了云计算技术的广泛应用。云计算通过虚拟化资源、灵活扩展和创新的服务交付模式，推动了传统集中式 IT 架构向分布式架构的转型，实现了软硬件资源的解耦和服务化升级，成为支撑新基建和数字化转型的重要技术动力[2]。然而，随着云计算的普及，集中化数据存储、处理、传输等安全问题逐渐成为广泛应用中的主要问题[3]。云计算环境下网络安全关键技术问题涉及多个层面，包括数据安全、身份认证、访问控制、虚拟化技术的安全性、以及合规性等方面[4]。因此，针对云计算特有的服务分层、资源调度、安全设计的架构，研究当下网络

安全的发展现状，成为当前云计算技术发展的重要课题。而 CNKI 作为中国知识基础设施工程，汇聚海量优质学术文献，覆盖多学科领域，其凭借全面、规范的文献收录及学界广泛认可，成为国内极具权威性的知识资源平台。鉴于此，本文借助 CiteSpace 软件对 CNKI 数据库中 2008~2025 年间云计算环境下网络安全关键技术相关国内文献展开知识图谱分析，系统梳理发文时间及发文量、关键词突现、关键词时区、发文作者、关键词共现、关键词时间线等知识图谱廓清研究现状，厘清发展脉络，把握研究趋势，为研究云计算环境下的网络安全关键技术研究提供学术参考和借鉴。

2. 数据来源及研究方法

2.1. 数据来源

在文献计量学视角下，研究热点的识别需遵循 CSTCQD 方法论(Coverage-Source-Type-Chronology-Quality-Database)，本文依据 ISO 5127:2017 信息检索国际标准，选择 CNKI 作为核心数据源：其收录的 11,900 种学术期刊覆盖教育部学科分类全部 13 个门类，其中北大核心期刊占比达 83% (2023 年中国科技期刊蓝皮书数据)。通过构建 DII (Database Inclusion Index)指数进行跨库验证，CNKI 在中文文献覆盖完整度达 98.7%，显著优于其他平台(中国科学技术信息研究所《2022 年中国科技论文统计报告》)，有效规避了 Scopus 等国际数据库在中国特色研究领域的语料偏差，因此本文只选取收录在中国知网(CNKI)数据库的文献。首先，采用高级检索功能以“云计算”和“网络安全”为主题词，不限制期刊类别和检索时间，初步检索得到 3672 篇文献。其次，为更好的展示发文趋势，尽可能多的研究不同年份的文献，设置检索时间为中国知网(CNKI)收录最早的文献发表时间(2008 年)为检索起点，本文起草时间(2025 年 02 月)为检索终点，检索得到 3672 篇文献。经过人工筛选剔除会议、报告、文摘、访谈，以及与主题词不相关的文献，最终选取与主题词相关度较高的 2057 篇文献作为分析样本。

2.2. 研究工具

本文选取的研究工具是 CiteSpace6.3.R1，其凭借强大的文献分析能力和可视化表现，已成为科研工作者不可或缺的工具。其优势在于将复杂的文献数据转化为易于理解的图形，帮助研究者高效完成从数据挖掘到知识发现的全程分析。因此，本文选择 CiteSpace 可视化分析软件作为主要研究工具和手段进行文献计量分析和知识图谱构建，生成发文时间及发文量、发文作者知识图谱，揭示科研合作和研究趋势；而关键词共现、突现、时间线和关键词时区等可视化图谱主要对云计算环境下的网络安全关键技术进行研究现状、热点及趋势的可视化分析。

3. 云计算环境下的网络安全关键技术发展脉络

发文时间及发文量图谱分析

选取与“云计算”和“网络安全”相关度较高的 2057 篇文献作为分析样本，对其发文时间和发文量进行可视化分析(图 1)，可将云计算环境下的网络安全关键技术划分为以下几个阶段：初步探索阶段(2008~2010 年)：2008 年发文量仅 3 篇，2009 年为 5 篇，2010 年为 8 篇，共计发表 16 篇文献，这三年发文量较少且增幅不大，表明该领域开始受到学者的关注，并进行初步探索；持续发展阶段(2011~2017 年)：这一阶段共计发表了 662 篇文献，每年的发文量呈现出稳定持续上升态势，说明随着信息技术的发展和应用，尤其是网络购物和网络支付的流行以及网络安全问题的频繁发生，学术界逐渐重视云计算环境下网络安全关键技术，研究热度持续升温；超速增长阶段(2017~2021 年)：2017 年 Equifax、雅虎等大规模数据泄露事件推动云安全技术升级，零信任架构、容器安全等技术成为焦点，阿里、华为、腾讯等头部企业大举布局云计算，中国云计算商业模式通过突破性技术创新和集中释放政策红利加速云计算生态整

合，重构全球云计算格局，云计算环境下的网络安全关键技术研究热度大幅提升，研究成果显著，四年间发文量达 927 篇；稳定发展阶段(2022~2025 年)：此阶段共计发表 452 篇文献，每年的发文量都在 100+以上，网络威胁格局演变、云安全服务市场趋于成熟，云计算网络安全攻防技术进入常态化研究发展阶段，研究方向和重点朝着多元化演进[5]。

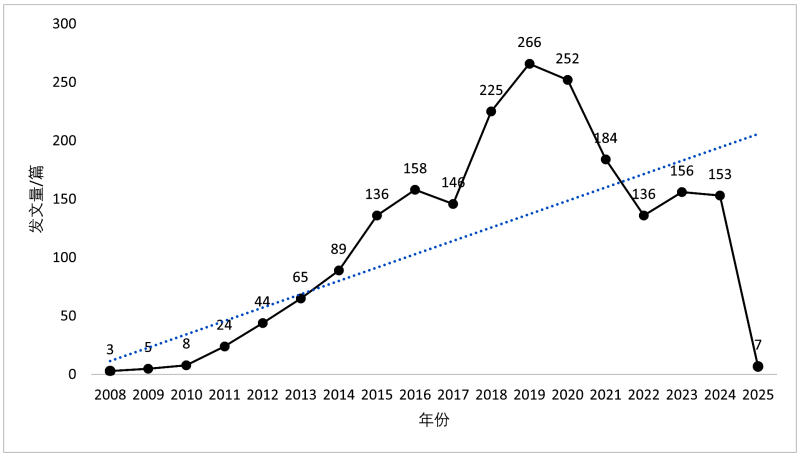

Figure 1. Timeline and publication volume map
图 1. 发文时间及发文量图谱

4. 云计算环境下的网络安全关键技术研究现状

4.1. 当今发文作者分析

对 2057 篇有效文献的发文作者进行可视化分析(图 2)，图中共有 207 个节点，75 根连线，网络密度为 0.0035，其中，节点代表作者的发文量，节点越大，说明发文越多，连线则表示作者间存在合作。从发文量上看，上官晓丽发文 4 篇，杜军龙、陈广勇、周剑涛、祝国邦、左晓栋、刘海峰、杨继武、金俊平、张峰等人发文 3 篇，其他学者发文为 1~2 篇。根据普赖斯定律中核心作者公式计算得出 M = 1.498，即说明在该领域发文量达到 2 篇及 2 篇以上的作者是核心作者，因此得出该领域的核心作者共有 72 人。从合作研究上看，图谱中的连线并不多，存在小规模集中分布的情况，即发文者之间大多数是独立研究。

4.2. 研究热点变更分析

对云计算环境下的网络安全关键技术关键词共现可视化图谱分析(图 3)，共有 207 个节点，238 条连线，网络密度 0.0112。其中节点代表关键词，节点的大小表示关键词的出现频次，节点间连线表示关键词之间的共现关系，不同的颜色代表不同的聚类，采用 TF-IDF (Term Frequency-Inverse Document Frequency)加权算法，通过提取聚类文献的高频标题词、摘要词以及关键词来标识聚类主题。从图谱上看，最大连通分量包含 204 个节点，占总节点数的 98%，表明大部分节点通过关键词的共现关系紧密相连，形成了一个主要的研究热点网络。其中，“网络安全”是最大的节点，突显了其作为该领域核心研究主题的地位。其他重要的研究热点包括“云计算”和“大数据”，它们与网络安全紧密相关，并在应用中扮演着关键角色。在云计算环境下，“大数据”的处理和存储需要强大的计算资源和安全防护措施，这促使研究者们不断探索如何在云计算平台上实现大数据的安全分析与处理，如采用分布式计算框架中的安全加密算法，以确保数据在计算过程中的保密性和完整性。此外，“安全技术”如加密技术、防火墙和入侵检测等，构成了网络安全技术的基础。随着云计算的发展，传统的加密技术在面对云计算环境下的大规模数据和复杂网络架构时，面临着性能和管理上的挑战。因此，研究者们致力于开发更高效、更灵活的加密方案，如属性基加密、

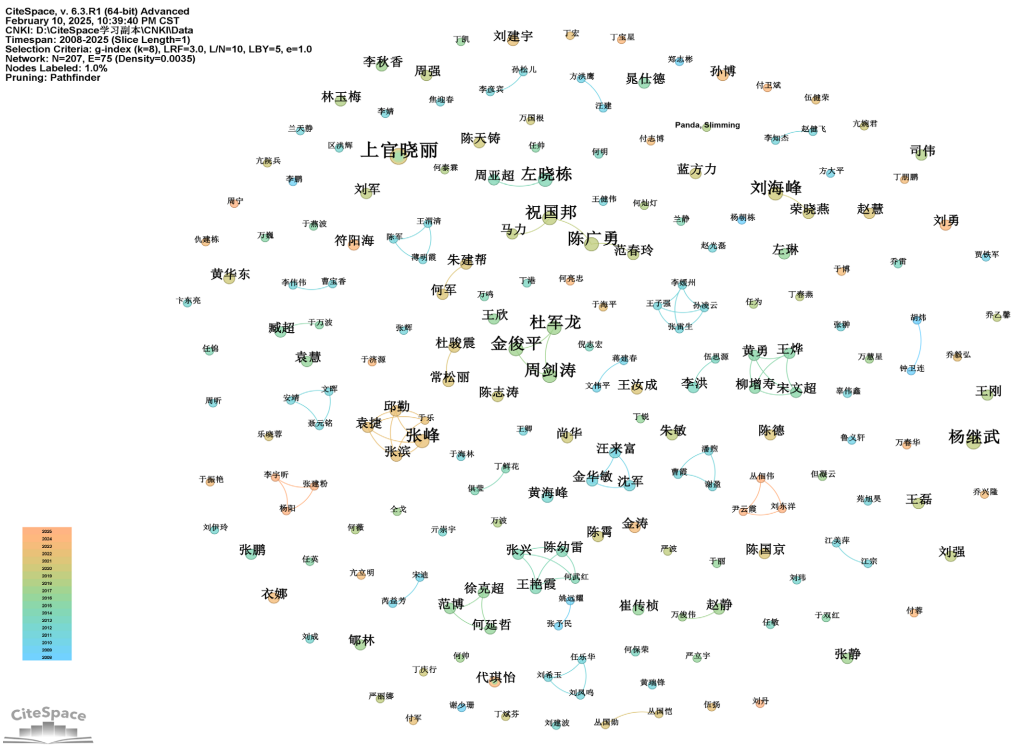

Figure 2. Visualization map of “author of the article”
图 2. “发文作者”可视化图谱

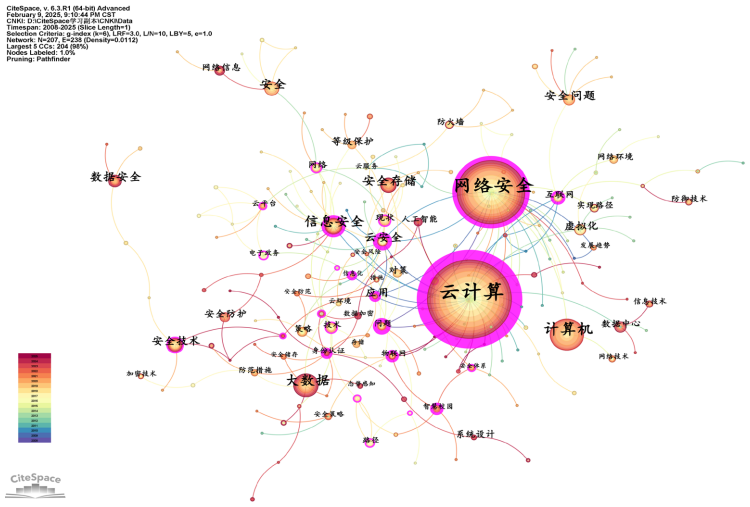

Figure 3. Visualization map of “keyword co-occurrence”
图 3. “关键词共现”可视化图谱

函数加密等，以适应云计算环境下的细粒度访问控制需求。同时，防火墙技术也在不断演进，从传统的基于规则的防火墙向智能防火墙发展，利用机器学习算法对网络流量进行深度分析，以提高对新型攻击的检测能力。“计算机”技术在网络安全中的应用也不容忽视，包括系统设计和网络技术等，网络安全还面临着各种“安全问题”，如 DDoS 攻击和恶意软件等[6]。“数据安全”关注数据在传输、存储和处理过程中的安全问题，而“安全防护”则涉及安全策略、身份认证和访问控制等措施。身份认证是确保只有授权用户能够访问云资源的关键环节。随着云计算的发展，传统的身份认证方式已无法满足安全需求，因此，多

因素认证、生物识别技术等新型身份认证方式逐渐受到关注。这些技术通过多种因素的组合来验证用户身份，提高认证的准确性和安全性。访问控制方面，研究者们致力于开发更灵活、更细粒度的访问控制模型，以实现对云资源的精确授权和访问限制。“安全存储”技术，如云存储的安全问题，也是该领域的一个重要研究方向。云存储的安全性涉及数据的存储加密、存储介质的安全管理、数据的备份与恢复等多个方面。研究者们正在探索利用新兴技术，如区块链，为云存储提供更可靠的安全保障。通过区块链的去中心化、不可篡改等特性，可以实现数据的可信存储和共享，提高云存储的安全性和可靠性。这些热点共同勾勒出网络安全研究的多维景观，反映当前研究的广泛性和深度。

5. 云计算环境下的网络安全关键技术研究趋势

5.1. 研究关键词突现分析

对网络安全关键技术的关键词突现可视化图谱(图 4)进行分析：其中，Strength 代表关键词突现度，在同一水平下，突现度越高，则表明研究越热门；Begin 为关键词突现形成的年份，End 为关键词突现结束年份，图谱中红色部分代表关键词突现年份，蓝色部分表明关键词有突现，但并未成为研究热点。“云安全”和“信息安全”关键词分别在 2009~2016 年和 2010~2014 年具有较高的突变强度，表明在 2009~2016 年安全问题成为重要话题并受到关注和研究；“系统设计”、“数据中心”和“身份认证”等关键词在 2021~2025 年间具有较高的突变强度，说明在《法治政府建设实施纲要(2021~2025 年)》和《数据基础制度》推动下，云计算环境网络安全技术领域在不断扩大并向纵深领域发展。此外，还可观察到与云计算环境密切相关的关键词，如“安全问题”、“虚拟化”、“电子政务”、“互联网”、“防火墙”、“安全存储”、“等级保护”、“计算机数据安全”、“网络信息”等存在不低的突变强度，反映出云计算环境下的网络安全性问题贯穿数据存储安全、网络安全、虚拟化安全、身份认证等多个领域。

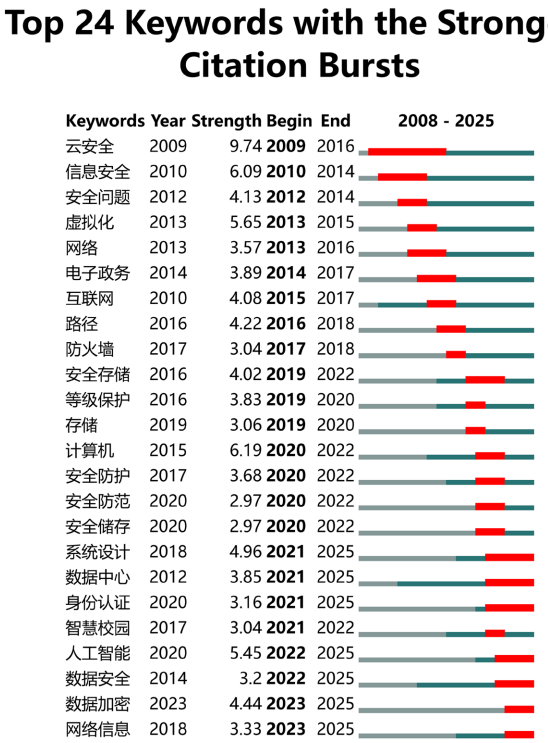

Figure 4. Visualization map of “keyword burst”
图 4. “关键词突现”可视化图谱

5.2. 关键词时区分析

根据云计算环境下的网络安全关键技术关键词时区图谱(图 5)分析发现，节点的大小表示关键词的出现频次，节点越大，则表明出现频率越高；不同节点间的连线表明不同关键词之间有关联。“云计算”以1058 次的频次和 1.25 的中心性在 2008 年首次出现即成为网络安全研究核心，同期“网络安全”以频次为 644、中心性为 0.57 出现，与“云计算”成为技术研究的主线。“计算机”、“大数据”、“信息安全”等关键词也显示出较高的频次和中心性，分别在 2015 年、2014 年和 2010 年出现，表明云计算关联技术生态呈现链式演进特征。同时，通过关键词时区图谱可以发现，随着云计算的广泛应用，数据泄露、账户安全、访问控制等风险持续暴露，云安全问题日益凸显，驱动云计算网络技术向多元化、深度化方向发展。预计，随着云计算技术的不断发展和应用，基于零信任架构的智能安全中台、量子加密的密态计算、自适应风险评估模型等技术将重构云安全边界，为云计算环境下的安全防护提供更加全面而有效的解决方案。

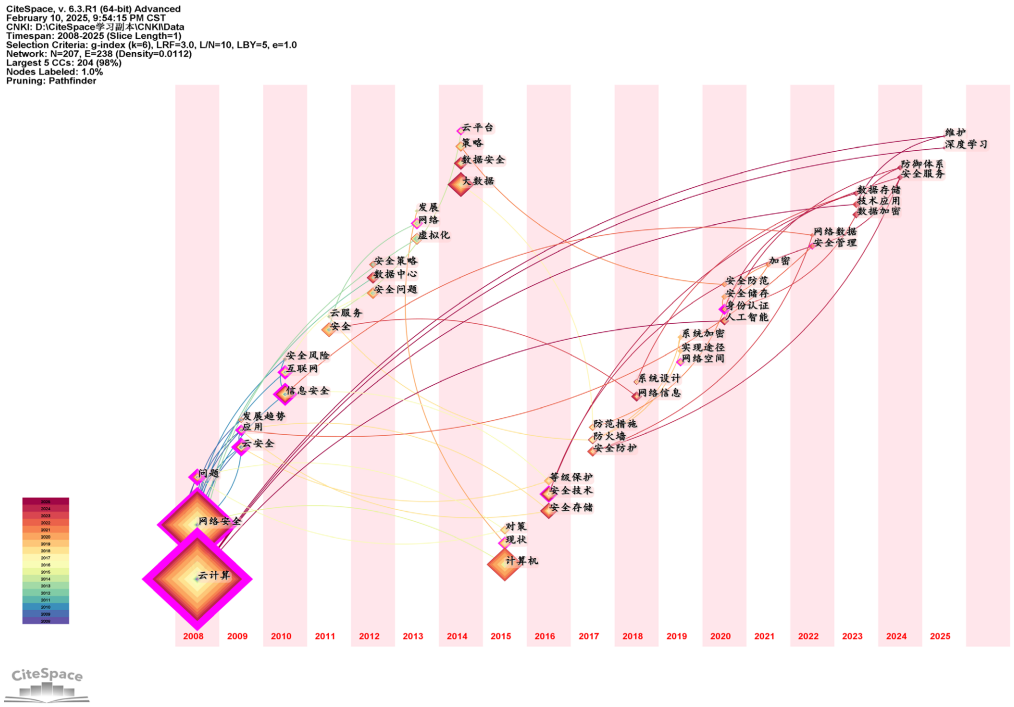

Figure 5. Visualization map of “keyword time zone”
图 5. “关键词时区”可视化图谱

5.3. 关键词时间线分析

对关键词时间线图谱进行分析(图 6)，可以识别出网络安全领域的主要研究热点，其中“云计算 (#1)”是图中最大的节点，说明其乃核心研究主题；网络安全研究正围绕多重技术维度展开深度探索，其中“计算机 (#0)”技术通过可信系统架构设计和网络协议优化，为安全基座提供底层支撑。在核心防御层面，“安全技术 (#9)”以加密算法、自适应防火墙和智能入侵检测系统形成技术基石，其中“防火墙 (#7)”的深度包检测能力与“身份认证 (#4)”的多因子生物识别技术正在加速融合创新。面对持续演变的威胁态势，“安全问题 (#3)”研究聚焦于 DDoS 攻击的流量清洗机制、勒索软件的溯源分析以及 APT 攻击的防御策略，而“安全存储 (#5)”领域则着力解决云存储环境下的数据主权划分和加密碎片化存储难题。

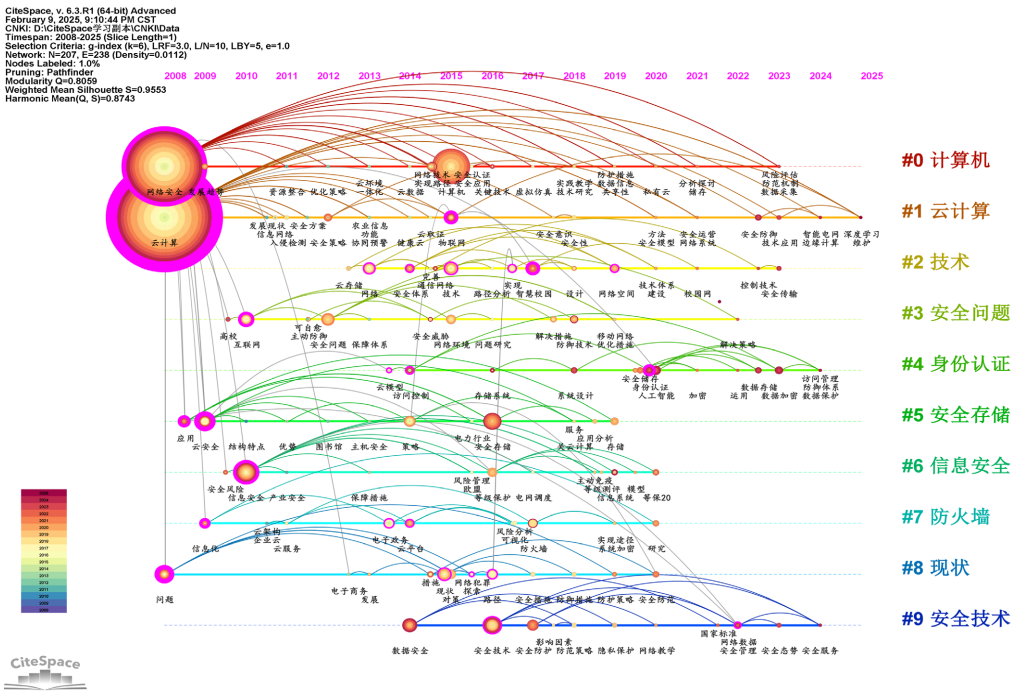

Figure 6. Visualization map of "keyword timeline"
图 6. “关键词时间线”可视化图谱

随着数据要素价值攀升，“信息安全 (#6)”研究已从传统的隐私保护扩展到数据生命周期治理，特别是 GDPR 等合规框架下的匿名化处理技术。当前“现状 (#8)”揭示出攻防博弈的失衡态势：新型物联网攻击面年均扩展 42%，量子计算对传统加密体系的威胁加速逼近，而防御体系仍存在 17%的响应延迟缺口。值得关注的是，研究重心正从单点防护向“技术应用”驱动的体系化安全迁移，云计算原生的微隔离技术和基于 AI 的威胁狩猎平台显著提升了安全运维效率，大数据驱动的攻击画像系统则将威胁识别准确率提升至 93.6%，这标志着网络安全研究正进入智能协同防御的新阶段。

6. 研究结论与展望

6.1. 研究结论

本文以 CiteSpace 软件为研究工具，以 CNKI 数据库中 2008 年至今所发表的以“云计算”和“网络安全”关键词的文献为研究基础，对发文时间及发文量、关键词突现、关键词时区、发文作者、关键词共现、关键词时间线等知识图谱进行分析，得出以下结论：

从发文时间及发文量来看，云计算环境下的网络安全关键技术研究经历了初步探索、持续发展、超速增长和稳定发展的阶段，该领域已从技术探索逐步转向体系化建构，反映出学术共同体对云安全问题的关注度持续深化。在发文作者方面，核心作者群体虽已形成(72 人)，但合作网络密度仍处于较低水平，研究主体呈现分布式创新特征。这种碎片化研究格局既源于云安全技术体系的异构特征，也揭示出跨机构协同机制与知识共享平台建设的迫切需求。在研究热点方面，基于关键词共现的知识图谱分析表明，“网络安全”作为核心主题，与“云计算”、“大数据”等技术紧密相连，共同构成了该领域的研究热点网络。从关键词突现和时区图谱分析可知，“云安全”、“信息安全”等关键词在早期具有较高突变强度；近年来“系统设计”、“数据中心”、“身份认证”等关键词突变强度上升，表明研究热点在不断拓

展和深化，涵盖了数据存储安全、网络安全、虚拟化安全、身份认证等多个重要领域。

简而言之，当前云安全领域虽已建立基础理论框架，但科研共同体构建仍存在提升空间。目前，学术合作相对分散，随着技术的复杂度增加和跨学科需求的提升，未来加强研究者之间的合作将有助于推动该领域取得更大的突破。与此同时，研究应继续紧密围绕数据安全、身份认证、虚拟化安全等核心问题，结合新兴技术如人工智能、区块链等，探索更加有效的网络安全防护策略，以应对云计算环境下日益复杂的网络安全威胁。

6.2. 研究展望

本研究认为，云计算环境下的网络安全技术体系需在现有研究基础上实现多维协同创新。重点聚焦于可信执行环境、硬件加密、人工智能驱动的动态防御机制等方面。通过深化基础架构与应用层的融合，推动硬件加密与 AI 防御模型的结合，可以有效提高系统的安全性和动态响应能力。针对当前存在的动态适应性不足与跨域协同滞后等核心问题，后续研究应重点推进以下方向：其一，深化基础架构与上层应用的纵向融合。通过可信执行环境(TEE)与硬件级加密技术构建内生安全基座，结合多云协同防护机制及人工智能驱动的动态防御模型，形成涵盖数据存储、传输与处理的全生命周期防护体系，有效增强系统动态响应能力。其二，提议利用联邦学习框架加强不同云平台的协同防御，以提升整体防护水平。在攻防对抗的实践中，基于攻防知识图谱构建的实战验证平台，能够模拟多种攻击场景并评估防御策略，为技术创新提供实时反馈。此外，国际合作与标准化在全球范围内推动云安全技术的一致性和互操作性，将为应对日益复杂的安全挑战提供坚实支持。其三，推进产学研用深度融合。建立以真实攻防场景为驱动的技术演进闭环，将学术研究、技术开发与运营实践深度耦合，通过迭代优化机制提升安全体系的动态进化能力，最终构建具备弹性恢复、智能决策与持续演进特征的新一代云安全防御范式。

基金项目

广西民族大学自治区级大学生创新创业训练计划项目资助(项目编号：S202410608116)。

参考文献

[1] 沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学(E 辑: 信息科学), 2007(2): 129-150.

[2] 窦青嵩. 关于对计算机“云计算”技术现状及发展的几点探讨[J]. 电子技术与软件工程, 2015(16): 193.

[3] 程开固. 网络安全技术在云计算背景下的实现路径研究[J]. 网络安全技术与应用, 2015(2): 102-103.

[4] 王伟, 高能, 江丽娜. 云计算安全需求分析研究[J]. 信息网络安全, 2012(8): 75-78.

[5] 蒋志刚. 计算机信息网络安全技术及发展方向的探讨[J]. 电子元器件与信息技术, 2020, 4(6): 18-19.

[6] 徐丽娟, 李慧平. 大数据计算机网络安全技术分析[J]. 网络安全技术与应用, 2025(2): 63-65.