项目结题验收单

专家验收表（主持人所在单位组织 3-5 名专家对项目进行验收、自评。）

项目名称	基于可信云计算的高校科学数据安全保障体系构建研究		
主持人	张宏亮	职务/职称	馆员/中级
所在单位	（加盖单位公章）吉林农业大学图书馆		
专家意见	2022 年，张宏亮主持的项目“基于可信云计算的高校科学数据安全保障体系构建研究”经 CALIS 全国农学文献信息中心审核并批准立项（项目编号 2022029）。该项目历时一年的研究，取得了预期的研究成果，现申请结题。专家组成员对该课题的研究过程进行了认真评议，形成如下验收意见： 1. 课题组成员能严格按项目申请时的要求开展各项研究。研究过程中，目标明确，研究方法选用合理，研究内容系统全面，工作严谨扎实，按时完成了预期目标，同意结题。 2 课题研究过程中注意搜集梳理相关文献，思路清晰，条理清楚，研究过程详细，内容详实，实用性较强，为高校科学数据安全管理、共享和使用提供一种快速有效的解决方案。该项目的研究既提升了研究人员科技创新的能力，又有助于提升科学数据的集约化管理与共享服务，实现科学数据价值最大化。 3. 该项目基于当前热门研究——科学数据的规范管理与数据安全，首先通过对国内外高校科学数据安全隐患、安全管理政策的调研，分析总结高校科学数据安全管理与开放共享的相关理论。其次项目实施过程中，课题组成员通过详细研究云计算数据安全威胁和问题，提出一种基于可信第三方云服务的解决思路，并深入研究了数据加密策略和秘钥管理以及可信第三方平台的运营模式等问题。之后课题组综合以上研究，构建以政府主导下的高校科学数据联盟为主体，可信第三方云平台为技术支撑，担负科学数据全生命周期安全管理；多方协同，形成政策保护下的高校科学数据安全保障服务体系。 （如需要可增加页数）		
专家签字			
职务/职称	研究员	副研究员	副研究馆员	研究馆员	教授

项目编号：
注:项目编号请查看立项通知，也可缺省

CALIS 全国农学文献信息中心研究项目

结题报告

项目名称：基于可信云计算的高校科学数据安全保障体系构建研究

项目关键词：科学数据 可信云计算 安全保障体系

项目单位（盖章）：吉林农业大学图书馆

通信地址：吉林省长春市新城大街 2888 号吉林农业大学图书馆

项目主持人：张宏亮

联系电话：18043179873

电子邮件：29085012@qq.com

提交日期：2023 年 5 月 24 日

基于可信云计算的高校科学数据安全保障体系构建研究

关键词： 科学数据 可信云计算 安全保障体系

1 研究背景、目的及意义

科学数据是国家科技创新和经济社会发展的重要基础性战略资源。国务院 2018 年 3 月颁布的《科学数据管理办法》，把“保障科学数据安全”列为首要任务。《科学数据管理办法》出台之后，国家有关部门和各省市自治区相继出台了各自的科学数据管理办法，以进一步加强和规范科学数据管理，保障科学数据安全,提高科学数据开放共享水平。可见，科学数据的重要性。高等学校是国家科技发展和技术创新的重要力量，其研究活动产生了大量的科研数据。但是高校的科学数据规范化管理尚处于起步阶段，海量的科学数据没有得到很好的管理和保存，科学数据的安全防护尤其薄弱。

随着大数据、云计算等信息技术的发展，互联网安全形势严峻，信息安全风险无时不在，科学数据随时面临着敌对势力、自然灾害、技术迁移等各种潜在安全隐患的威胁。面对这种安全形势，如何保护高校科学数据的安全使用，服务于国家科技创新、经济社会发展与国家安全，构建高校科学数据安全保障体系就成为当务之急，也是长远所需。

1.1 国内外相关研究综述

（1）科学数据安全管理研究

1960 年美国国家大气研究中心对地球科学数据进行建模、收藏和保存，开始引发众多国家和学者重视科学数据。20 世纪 70 年代，数据载体由纸质转为数字，世界各国的科学数据中心应运发展，迎来了科学数据建库时代。我国以中科院为中心建设科学数据库，20 世纪 80 年代研究、立项、起步，90 年代科学数据建库步入高潮。这一时期的研究主要集中在系统平台的稳定运行和数据保存。

21 世纪初，Web 技术的广泛应用，科学数据在互联网上开放共享，安全风险扩大，数据安全上升到各国国家安全层面。我国 2001 年开始，Web 技术应用于科学数据库门户网站，到 2008 年 6 月，科技部科学数据共享平台，整合资源总量 35.5 TB，数据库 3616 个，负载和源于网络的安全事件频出。这一时期，科学数据安全转向动态防护，进入了网络安全研究阶段。

2006 年 Google 提出云计算概念，2011 年美国国家标准技术研究院确立了云计算定义。2012 年，从数据安全角度研究云计算，热度持续至今。我国科学数据共享平台，到 2015 年底有 655TB 科学数据为用户提供云服务，科学数据安全研究向云时代深度防护发展。

（2）科学数据开放共享研究

科学数据开放共享在理论、实践及技术应用等方面成果颇丰，具体包括：①科学数据共享的理论研究，包括科学数据共享的理论依据、共享动力、共享障碍、共享机制、共享框架、科学数据涉及不同主体的角色、共享管理系统的主控因素及相互作用等。②基于学科分布，对生物、医学、基因学、化学、地理科学、心理学、统计学、经济学等众多学科领域的科学数据共享及服务、相关数据平台、数据中心等的理论与实践研究。③科学数据共享涉及相关技术的研究，包括本体技术、元数据描述及互操作、关联数据和语义网等新的信息组织技术、对科学产出影响的量化分析技术等。

（3）信息安全保障体系研究

信息安全保障研究，经历了从通信安全、计算机安全、信息系统安全到信息安全保障等阶段演变，涌现出《保密通信的信息理论》、《可信计算机系统评估标准》、安全体系结构概念、《信息保障技术框架》(IATF) 等成果。其中 IATF 对国内外信息安全保障系统建设影响深刻，为科学数据安全保障研究提供了依据。

总结：基于以上分析可以看出，有关科学数据安全保障研究是国内外研究的热点，也是各个国家、研究机构关注的焦点。虽然国外相关的研究比较成体系，但国内的相关研究比较分散，还是没有形成一个体系，尤其是从高校角度进行的有关科学数据的安全保障体系的研究成果就更少。为此，本课题提出一种可信云计算平台为支撑、数据联盟为主体的高校科学数据安全保障与服务体系构建思路。

1.2 课题研究目的与意义

（1）高校是科学数据的主要产出者，也是科研资助机构资助项目的主要承担者，课题的研究可以实现高校科研数据的集约化、汇交、管理和共享服务，实现科学数据价值的最大化，进而推动国家科技创新和社会经济的发展。

（2）课题基于可信云计算安全技术理论，协同多方的力量，为高校科学数据安全保障体系建设提供了一个低成本、高可靠的全新解决方案。

（3）课题把科学数据纳入到图书情报学的研究范畴内，进行科学数据的安全管理、开放共享与应用服务等的研究，并提出了全新的高校科学数据安全防护体系构建模式，是图书情报学理论的极大丰富。

2 研究内容及方法（思路、方法、具体内容）

2.1 研究的思路及方法

课题从分析高校科学数据安全现状及潜在安全风险和现实问题入手，通过调研国内外高校科学数据安全管理相关研究成果的跟踪，构建高校科学数据安全管理内容框架。在探讨云计算数据安全问题的基础上引入可信云计算理论，研究数据安全技术与策略以及运行模式，从而构建以政府主导下的高校科学数据联盟为主体，可信云服务平台为支撑，担负科学数据全生命周期安全管理的高校科学数据安全保障与服务体系。

课题以信息安全研究常用的量化分析法、文本分析法为主，以文献调研、专家评估法等为辅助，采用多种研究方法达到研究目的。

2.2 研究的主要内容

本研究通过抽取 U. S. News 世界排名前 50 的 47 所高校图书馆网站为调研对象，分析高校科学数据的安全现状及其潜在的安全风险，结合国内高校的组织结构，以科学数据全生命周期安全管理政策，归纳了高校科学数据安全内容框架。总结分析了大数据安全保障体系、云计算安全技术及其优缺点，并引入可信第三方云服务提供商，分析，调研，研究了可信云第三方服务平台的关键技术、安全服务、运营模式等。在上述调查研究、量化分析、模式构建的基础上，明确了高校科学数据中心、云计算企业、科研人员等各自的角色、任务和相互间的关联机制，最终形成了一个科学严谨、具有可操作性的“基于可信云计算的高校科学数据安全保障体系”的总体构建方案。

3 结论与建议

3.1 高校科学数据安全内容框架

以科学数据安全为出发点，选取 U. S. News 世界排名前 50 的高校图书馆网站作为调研对象，最后实际调研 47 所高校，提取这些高校科学数据管理政策中关于科学数据安全的内容，在此过程中发现科学数据安全内容围绕责任主体展开，因此结合

我国高校部门设置现状，确定科学数据安全内容框架中的责任主体。高校关于科学数据安全相关责任主体的职责大致按照科学数据生命周期划分，所以本文综合了学界认可度较高的科学数据生命周期，确定了本文科学数据安全内容框架中科学数据生命周期的阶段。最后研读以上高校科学数据安全管理内容，通过语义层面的归纳总结生成科学数据安全内容框架。

经过对以上 47 所高校科学数据管理文本分析，科研人员、科学数据存储库是高校科学数据安全相关的主要主体；为校内人员提供科学数据存储的选择、科学数据风险评估、科学数据脱敏是保护科学数据安全的主要途径；科学数据生命周期的每个阶段都与数据安全有关，着重在数据描述阶段、数据存储阶段、数据开放阶段。

科研人员是高校科学数据安全政策的主要执行者与落实者，结合国内高校组织结构设置，构建出适合我国高校制定科学数据安全管理的内容框架，该框架所有主体均围绕保护科学数据实现运转，主管部门独立于其他主体之外，主要从宏观角度把握科学数据，为保护科学数据安全制定政策，监督高校、科学数据存储库管理科学数据安全情况。高校属于中观层面的主体，起到承上启下的作用。科学数据存储库与科研人员是执行者，是微观层面的主体。科研人员主要执行高校的相关政策，为科学数据存储库提供科学数据，同时，管理保存科学数据。

3.2 基于可信第三方的解决方案

在云端数据安全储存中，有大量模块需要独立于云端运行。为此，课题组引入一个“可信第三方”的概念，在云端数据储存中，通过可信第三方的运作，将一部分原本由云端承担的工作独立出来，运行一些独立的模块，分摊部分用户数据资料，从而保障云端数据安全。

3.2.1 可信第三方设计思路。在电子商务等领域，可信第三方的概念早已被广泛应用。在当今云计算背景下，很多用户对云服务提供商展现出不信任的情绪，却又有相关需求不得不使用其提供的服务。由于云服务特殊的架构，云服务提供商权力过大过于集中，让用户产生一种本能的不信任感。在这种情况下，引入可信第三方的概念，通过可信第三方平台承担云的部分工作，削弱云服务提供商权限，并通过特殊的工作机制对云服务管理员产生一定的监督作用，同时分担了风险，不会因为云平台被攻破而造成数据泄露。

3.2.2 可信第三方平台运营模式

可信第三方平台的运营主要有两种模式。针对个人用户及小型高校来说，可以由有实力的第三方互联网公司提供专门的云平台第三方服务。如同“支付宝”这类第三方支付平台一样，终端用户甚至不需要为第三方服务支付任何服务费用，因为云服务提供商将为吸引用户而承担可信第三方服务费。针对大型高校、政府机构来说，如果对保密性要求更高，或是希望能更好地掌控自己的数据，也可以自行搭建第三方平台，将其置于高校防火墙内，通过更严格的管理制度与更完善的技术保障，做好全面防护。

3.3 高校科学数据安全保障体系

综合以上调研分析，本研究提出以高校科学数据联盟为主导，科学数据中心为主体；与可信第三方云服务提供商合作，担负科学数据全生命周期安全管理；在数据安全内容框架、政策法规的基础上明确数据联盟，可信第三方云服务提供商和科研人员等各自的角色、任务和相互间的关联机制，最终形成一个科学严谨，具有可操作性的，多方协同的高校科学数据安全保障体系。

3.4 成果存在的不足，需要深入研究的问题

高校科学数据安全保障体系构建是个大课题，也是信息安全中的难题，业内对此问题非常敏感，数据采集取证非常难，课题组成员在调研过程中进行了不懈努力，由于多方面能力所限，研究成果还存在以下问题。

（1）基于可信云计算的高校科学数据安全保障体系构建方案需要进一步在实践中检验、完善和补充，尤其是后续的管理模式、运行机制、服务规范等等，还需要继续跟进研究。

（2）云计算企业的优劣还没有统一的评判标准，在方案的应用过程中，要对云计算企业进行更深入的调查研究、评估，选取集成能力强、规模大、社会反响好，列入国家信息安全战略计划的企业，作为合作伙伴。

（3）对国内高校科学数据安全管理的调研过程中，由于涉及到管理问题、数据保护问题、商业机密等原因，只是依据考察、访谈、网站调研进行了定性研究，定量研究不够，需要继续深入研究。

4 项目成果（发表的文章、开发的软件、取得的实践效果等）

5 参考文献

[1]刘敬仪,江洪.开放科学环境下国外高校图书馆科研数据管理服务启示[J].图书馆工作与研究,2018(10):18-24.
[2]中华人民共和国科学技术部.科技部财政部关于发布国家科技资源共享服务平台优化调整名单的通知[EB/OL].[2022-4-17].
[3]中国科学院计算机网络信息中心.《科学数据安全技术及基础技术标准研究》项目工作部署视频会议顺利召开[EB/OL].[2022-4-17].
[4]Committee J I S.Security of researchdata[EB/OL].[2022-04-18].
[5]国家科技基础条件平台中心.国家科学数据资源发展报告（2017）[M].北京:科学数据文献出版社,2018.
[6]王熊.网络空间国家大数据主权安全危机治理研究[D].南京:南京师范大学,2018.
[7]中国政府网.习近平总书记在网络安全和信息化工作座谈会上的讲话[EB/OL].[2022-04-18].
[8]李大光.我国科技安全面临的挑战和战略思考[EB/OL].[2022-04-18].
[9]温亮明,张丽丽,黎建辉.大数据时代科学数据共享伦理问题研究[J].情报资料工作,2019,40(2):38-44.
[10]Best global universities rankings [EB/OL].[2020-06-28].ht-tps://www.usnews.com/education/best-global-universities/rankings.
[11]University of London [EB/OL].[2020-06-28].https://lon-don.ac.uk/search?search=research+data.
[12]Sorbonne University [EB/OL].[2020-06-28].http://www.sorbonne-universite.fr/.
[13]Sydney University.Archive research data [EB/OL].[2020-07-01].https://library.sydney.edu.au/research/archiving-data.html.
[14]Johns Hopkins.Data services [EB/OL].[2020-07-01].https://dataservices.library.jhu.edu/training-workshops/research-data-management-sharing/effectively-managing-and-sharing-research-data-in-spreadsheets/.
[15]Cambridge University.Data management guide [EB/OL].[2020-07-01].https://www.data.cam.ac.uk/data-management-guide.
[16]Harvard University.Harvard research data security policy(HRD-SP)[EB/OL].[2020-07-01].https://vpr.harvard.edu/pa-ges/harvard-research-data-security-policy.
[17]Imperial College London.Research data management [EB/OL].[2020-07-01].http://www.imperial.ac.uk/research-and-in-novation/support-for-staff/scholarly-communication/research-data-management/.
[18]Nanyang Technological University.Research data management:Home[EB/OL].[2020-07-01].https://libguides.ntu.edu.sg/rdm/intro.
[19]Shameli-Sendi A.An efficient security data-driven approach for implementing risk assessment [J].Journal of Information Securi-ty and Applications, 2020, 54(Oct.):1-18.
[20]Patel K, Jethava G B.Privacy preserving techniques for big data:A survey [C]//Proceedings of 2018 2nd International Confer-ence on Inventive Communicationand Computational Technolo-gies.Coimbatore, 2018:194-199.

[21]Song H,Wang N,Sun J,et al.Enhanced anonymous models for microdata release based on sensitive levels partition[J].Com-puter Communications, 2020, 155(Apr.):9-23.
[22]穆良，程良伦.基于k-匿名位置隐私保护的自适应学习模型[J].计算机工程与应用，2017，53(18):89-94，101.
[23]叶云，石聪聪，余勇，等.保护隐私的分布式朴素贝叶斯挖掘[J].应用科学学报，2017，35(1):1-10.
[24]周倩伊，王亚民，王闯.基于互联网大数据的脱敏分析技术研究[J].数据分析与知识发现，2018，2(2):58-63.
[25] Huang H P, Zhu P, Xiao F, et al.A blockchain-based scheme for privacy-preserving and secure sharing of medical data[J].Com-puters & Security, 2020, 99:10-22.
[26] Virginia G.Data sharing:An open mind on open data[J].Na-ture, 2016, 529(7584):117-119.
[27]杨燕,阮建海.基于科研过程的科学数据安全行为研究[J].知识管理论坛，2019（4）: 218-231.
[28]李善青,郑彦宁,邢晓昭,等.科学数据共享的安全管理问题研究[J].中国科技资源导刊，2019,51（3）: 11-17.