网络出版时间：2019-06-11 09:27:57
网络出版地址：http://kns.cnki.net/kcms/detail/11.3792.G4.20190611.0841.036.html

文章编号:1006—9860(2019)06—0123—08

信息安全技术在教育数据安全与隐私中的应用分析*

刘梦君[1]，姜雨薇[1]，曹树真[1]，杨 兵[2]

(1.湖北大学 教育学院，湖北 武汉 430062；2.湖北大学 智慧学习研究中心，湖北 武汉 430062)

摘要：合理运用信息安全技术保障教育用户在教育网络空间上的数据与隐私安全，事关网络空间国家主权安全、教育用户人身和精神基本人权安全。该文从教育视角下的信息安全技术体系出发，解剖了教育安全与教育数据安全的辩证关系，阐明了教育数据安全与隐私的内涵与特点；梳理了有关教育数据安全与隐私保护的当前研究进展与现状；明确了教育数据安全与隐私保护目标，并针对性地总结一般应用信息安全技术进行教育数据安全与隐私保护的流程；指出了信息安全技术在教育数据安全与隐私保护领域深入应用面临的挑战。最后展望了信息安全技术教育应用发展方向。

关键词：教育信息化；教育信息系统安全；教育数据安全与隐私；学习安全与隐私

中图分类号：G434 **文献标识码：**A

一、引言

经过政府和业界多年不遗余力地推进教育信息化，大量存储在网络空间上的教育信息系统用户的个人隐私数据，带来诸多意想不到安全威胁，引起了各方的高度关注。《中华人民共和国网络安全法》的颁布，标志着对网络空间上的信息系统安全的重视已经上升到国家战略。教育作为国运兴衰之所系，其在网络空间上的安全保障重要性不言而喻。美国政府为此颁布诸如《家庭教育权和隐私权法案》等一系列法典，严格保障学习者数据与隐私安全[1]。微观上，围绕如何在网络空间中保护学习者个人数据和隐私安全[2]，国内外研究者在各个层面进行了探讨。李青和李莹莹从管理手段出发，提出了立法、伦理约束、行业自律、政府监管等对应策略，以促进形成良好的数据利用氛围[3]。杨现民等认为要加强教育数据安全与运营监管[4]，并系统地提出从体制、机制、技术、方法等多个层面制定《教育大数据安全管理办法》的管理细则[5]。Pardo等提出同时从法律和技术层面来保障学习者对数据的控制权，控制数据的访问权，明确问责机制和评估原则[6]。法律层面，徐鹏等指出应该从法律出发来保护教育大数据的安全，限制如今各类教育数据挖掘技术和学习分析技术的滥用[7]。伦理层面，Rubel等认为在进行学习分析时要充分考虑到伦理问题，在教育数据的采集上必须明确数据的收集范围和保障学习者的自主权[8]。技术层面，李青等提出以区块链技术对于推动教育的开放和公信力，构建去中心化安全的全球知识库[9]。虽然不同的研究者提出解决问题的策略及角度不尽相同，但都认为从技术手段保护学习者的个人数据和隐私安全十分必要。

从技术角度来看，教育数据安全与隐私可从数据与学习者关联程度分为4个层级。如图1所示，第一层是数据的物理存储媒介安全，如存储设备的防灾防盗等；第二层是存储设备本身系统运行功能的安全，如操作系统的安全；第三层是数据内容安全，包括数据不被外界篡改、删除，数据内容表示的教育信息不被外界知晓；以及最上面的第四层，

图1 教育信息系统安全技术层级体系

* 本文受国家自然科学基金面上项目“面向移动位置服务的空间位置大数据差分隐私保护研究”(项目编号：41671443)、湖北省自然科学基金课题“移动环境下安全的位置服务关键技术研究”(项目编号：2017CFB136)资助。

数据内容隐含的学习者隐私等背景信息不被泄露。而在网络空间中，最容易威胁到学习者个体的便是三、四层上的数据及隐私泄漏安全，这也是本文论述的信息安全技术关注的重点。

二、教育数据安全与隐私的问题及内涵

(一)教育数据安全与隐私问题的产生

教育数据安全与隐私风险产生的根源来自于教育信息化。早期的教育数据类型多为静态数据，形式和内容较为单一(一般仅为学习者的个人学籍和成绩等教学管理及教育活动产生的数据信息)，信息化程度低，加之人们对个人信息安全可能会造成的不良影响没有充分的认识，因此，对于教育数据的安全与隐私问题关注度低。进入互联网时代尤其是移动互联网时代以来，移动通信技术、物联网、Web2.0技术等快速发展。一方面，越来越多的学习资源被投放到网络平台上，学习者们在使用平台学习时，留下了大量的个人和学习记录信息。如此高信息量的学习者数据，会引发一些别有用心之人窃取数据用于非法用途的心思。另一方面教育数据隐含着学习者的行为、方式、成果、动机等等零碎的信息，当采用合适的数据分析与挖掘技术时，这些零碎的信息就会相互作用和组合成新的更有价值的数据链，产生学习者本身都意识不到的隐私。

然而，解决教育信息化过程中的安全问题并不能照搬现有信息系统的安全保护技术措施。作为信息技术的一种行业应用，教育信息系统在同样存在着其它信息系统面临的安全问题的同时，还面临着如下几方面的相对特殊的问题：(1)信息安全保障人才相对缺乏问题。广大乡村、偏远落后地区的教育信息系统因为规模小，所配属信息维护人员多由未受过专业培训的教师兼任。这种人才资源上的不足，很容易使得信息系统受到入侵和破坏，泄露和污染学生数据。(2)用户安全经验缺失问题，教育信息系统的用户多是未成年或涉世不深的学生，因而更容易被别有用心之人利用诸多欺骗手段窃取敏感信息。(3)管理者安全意识淡薄问题。目前的教学及管理人员普遍缺乏安全意识，未能充分认识到学生日常的个人、生活、学习记录对学生信息安全的重要性，导致在不经意间泄露了学生敏感信息。这几方面的问题，很大程度上，并不能通过管理、自律、法律法规手段完全解决，必须使用技术手段补足支撑。

(二)教育数据安全与隐私的理论内涵

由于信息已经成为经济社会发展的一项重要战略资源，事关一国网络空间主权安全，各国对于网络空间上信息的获取、使用及控制十分严格。信息系统的安全问题最早源自微型计算机系统安全，随着计算机网络的发展，安全边界拓展到了网络空间上。Blakley等[10]对于信息安全的定义是：防止对数据未经授权的访问、使用、披露、破坏、修改和删除。信息安全的目标是在保障数据的机密性和完整性的同时，保持数据的可用性，而信息安全技术是指为了达到上述信息安全目标而采取的一系列技术手段。

相对于信息系统的安全，教育领域中一直就有安全的概念。早在2005年，教育部就向各高校、中小学下发了《教育系统突发公共事件应急预案》。预案中教育安全的内容包括：自然灾害安全、事故灾难安全、公共卫生安全、突发社会安全、考试安全这五大安全。前四项对应着人身安全、后一项对应着教育信息系统用户数据安全。而随着信息化的推进，一方面前五大安全都进行了信息化改造；另一方面许多教学活动也迁移到信息系统上开展，于是，网络与信息安全亦于2015年被增补进应急预案中。由此可见，教育安全一直是教育管理部门关注的重点，只有切实保障教育用户在教育信息系统全过程的安全，才能更好地开展后续教育活动。

在教育信息系统中，信息安全技术无论是在用户人身安全层面，还是在用户数据安全层面，都有着重要作用(如图2所示)。这两个层面的研究都是为了更好地让学习者拥有安全的受教育环境。所不同的是，前一个层面的安全观念因为影响直接、继承诸多传统观念，因而能够被人们感同身受。而后一个层面的安全，概念上较为抽象，直观上不易接触，需要通过一定的事件，才有可能对外呈现。因而在人们的观念当中，对其严重性认识多有不足。而这种认识上的陌生，一旦出现安全事件，将会借助信息化平台快速传播，造成全社会范围内的恐慌。因而，信息安全技术在学习者数据安全层面上的应用，不仅是推动教育安全的必要保障，亦是推动网络空间安全这一虚拟空间主权观念在广大国民认知中的一个重要契机。

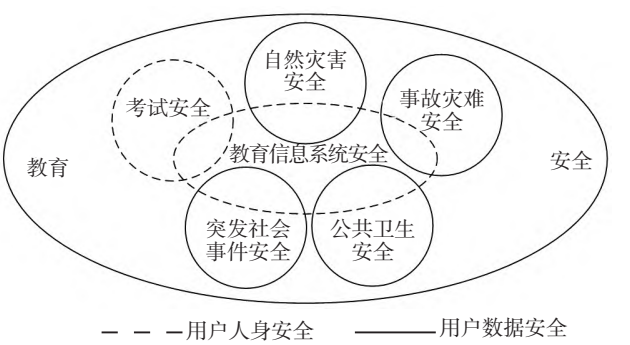

图2 教育安全与教育信息系统安全概念关系

三、教育数据安全与隐私保护典型技术及应用研究现状

(一)教育信息系统安全保障可用的典型信息安全技术

目前常用的信息安全技术包括接入控制技术、攻击防护技术、加密技术、隐私保护技术等[11]，如下表所示。随着网络空间内的安全攻击类型越来越复杂，研究多技术合成、抗攻击能力更强的信息安全技术，成为新的安全技术发展趋势，也是高起点保障教育信息系统安全新的契机。

典型信息安全技术的分类表

防护类型	主要技术	技术特点	用途
接入控制	防火墙	过滤掉所有未授权的外部设备的网络连接请求	阻止未授权的外部网络设备接入系统
	身份认证	验证用户身份是否与预设信息匹配	阻止非法用户进入系统
攻击防护	入侵检测	收集系统运行记录而后分析其中违反安全策略的行为	检测出信息系统内的异常程序行为
	杀毒技术	对检测到的异常程序进行隔离和删除	阻止并清除系统内恶意程序
数据加密	Hash(散列)函数	同一原始数据生成固定长度且内容相同的摘要	确保大文件的完整性
	对称加密	加密者和解密者使用相同的密钥	确保数据的机密性
	非对称加密	加密和解密数据分别使用不同的密钥	确保大文件的完整性 机密性及不可抵赖性
隐私保护	匿名技术	同一属性值数据记录至少有2项以上	保护单一用户真实属性值隐私
	泛化技术	减小用户属性值数据的精度	
	扰动技术	在用户属性值上添加随机数值	

(二)信息安全技术教育数据安全与隐私保护应用研究现状

国内外关于教育数据安全与隐私的研究多侧重于伦理道德上的剖析，从技术视角分析教育数据安全与隐私的研究不多，且较为零散。通过对相关研究进行整理和分析后发现，当前使用信息安全技术对教育信息系统的安全与隐私的相关研究主要分为以下五个方面。

1．教育信息业务系统数据安全模型研究

理想中安全的教育信息系统应该不具有任何安全短板。按照教育数据安全使用周期内的要求，从底层的网络接入，到系统运行，到数据存储，传输乃至应用全流程都应该进行完备的安全防护。但在具体的教育业务系统，需要根据业务系统自身的安全需求，进行安全功能上的精心取舍，因此具体的安全模型和框架就需要研究者和业界因地制宜进行设计。研究者们分别根据移动在线学习[12]、教育云[13]、教育大数据分析[14]、教育区块链[15]上业务系统的安全风险和安全需求设计了一系列针对性的安全模型和框架。

2.教育信息系统文件安全保障方案设计研究

教育信息化普及深入，推动各教育相关机构办公朝着无纸化、无介质化方向稳步发展。但无纸化的发展，使得教育活动文件脱离了主管单位物理控制，产生了文件滥用，权限失控，版权不明，内容失真等诸多问题。对于教育活动文件安全，研究者们重点关注了跨高校学生档案文件共享安全[16]，高校学生电子学历文件安全[17]，学生作业和教师评阅后的文档存在的篡改和泄露学生隐私问题[18]等几方面问题。

3.在线学习系统的数据安全与隐私保障技术研究

在线学习改变传统的师讲生学的教学模式、摆脱了传统教学受固定时间、地点、学习过程单向和串行授课的约束，使得碎片化学习、协作学习、泛在学习、终身学习成为可能。但从知识产权、数据安全和学习者个人隐私角度来看，在线学习又将学习者和教育机构推向了危机的前沿。围绕着保障在线学习安全与隐私，研究者们使用信息安全技术一方面进行了接入应用系统的用户身份验证，确保只有合法的用户进入在线学习系统。使用技术从简单的静态口令[19]，动态口令[20]，到复杂的生物特征[21]，乃至最新的区块链技术[22]。另一方面则对进入系统使用过程中的数据安全[23]与个人隐私保护展开了相关研究[24-27]。

4.在线考试系统安全保障技术研究

在线考试系统的出现，极大简化了考试准备工作，大幅提高了后续的批阅、统计、分析和存档管理效率，将会成为未来智慧教育的重要组成部分，但它面临着试题和考生答题内容被泄露和篡改，考生作弊的问题。因此在线考试系统的安全研究工作主要围绕两方面展开，一是通过各种身份验证技术验证应试者是考生本人，防止作弊[28][29]；二是使用试题数据加密和签名技术，保证试题和考生答卷内容的机密性和完整性[30][31]。

5.学习数据分析与挖掘中的安全与隐私保护技术研究

学习数据分析与挖掘对于后续学生的培养发展，提高教学质量，并应用于各类奖惩计划有重要作用。但学生记录数据涉及到个人隐私，不能简单对外公布。因此如何在保护学生个人隐私同时，对学习记录数据进行有效挖掘，成为摆在推动学习数据挖掘前的主要问题。学习数据隐私挖掘经历了一个经验安全到理论安全的过程。在第一阶段的经验

安全保障阶段，使用各种匿名技术，对学习数据中个体敏感属性进行匿名化处理[32]。随后，伴随着隐私保护技术的发展，理论安全的差分隐私技术被提了出来并应用到了各类学习数据挖掘应用当中[33]。

四、基于信息安全技术的教育数据安全与隐私保护

(一)信息安全技术保障教育数据安全与隐私的模型

典型教育信息系统里面包含着学习者、教师、教学管理人员和系统运维人员4方面用户。这4方面用户对于教育数据而言既有可能是合法用户，也有可能是安全威胁。教育数据安全与隐私保护的目标是通过接入控制、攻击防护、数据加密、隐私保护等信息安全技术：在学习者合法使用教育信息平台的同时，保护学习记录和个人信息等数据安全的隐私，同时阻止和检测出对他人数据的非法访问；为教师提供合法的信息化教学辅助的同时，防止其教学资源和成果被人非法窃取，并尽可能减小其对学生数据有意无意的非法获取；为管理人员提供合法的信息化管理辅助同时，阻止并检测出其有意无意间泄露用户数据及隐私；为系统运维人员提供维护系统接口同时，阻止并能检测出对教育业务数据的访问记录。简而言之，让上述4方用户在保障教育数据安全同时，依然能够开展正常的教、学、管、维活动，形成一个教育数据安全共同体。

(二)信息安全技术保障教育数据安全与隐私的框架

信息系统安全遵循木桶理论，即系统的安全程度高低由最薄弱环节决定。因此，理论安全的教育信息系统任一环节上的安全都需要得到最大化的加强。一个安全的教育信息系统需要解决三个环节上的安全问题，即：安全地“采和传”、安全地“存”、安全地“用”。即系统内的数据生成及流动过程中不被泄露或非法篡改，存放在系统期间不被泄露或非法修改，使用时候不被泄露或非法篡改。具体保护流程如图3所示。

在教育数据采集和传输过程中，需要根据所面临的安全威胁，来决定使用一种或者几种信息安全技术的组合，构建安全的数据采集与传输方案。当想阻止可靠的设备传输数据内容被泄露时(如音视频设备录制数据，固定点采集活动数据)，通常由交互发起方使用对称密钥，对交互数据进行加密后发送给另一方。当想阻止篡改通信数据或者抵赖数据来源时(如学习者准备提交给系统的学习行为数据)，则由交互发起方，使用基于哈希函数和非对称加密技术的数字签名技术，对交互数据生成签名，另一方则使用交互发起方公开密钥，验证签名来判断原始数据有无被篡改。如想同时防止数据泄漏和数据被篡改(如学习者的个人资料数据)，则由交互发起方先对原始数据使用对称密码加密，然后使用哈希函数生成摘要，再使用非对称的私密密钥生成签名，然后将密文和签名一同发送给交互另一方，另一方验证签名后再解密数据。以上数据泄漏都是针对有权限接触到用户数据的管理者外的人员，如果还想防止个人敏感数据(如教学评价数据，投票调查数据)被管理者知晓，则需要使用个人隐私保护技术对个人敏感数据进行隐私消除处理，再传输给平台。

在教育数据存储安全保障中，需要根据系统自身所拥有的资源来决定使用一种或者几种信息安全技术的组合，构建安全的数据存储方案。当教育信息系统主管单位有充足资源时(如大型高校和大型在线教育平台)，一般自建硬件平台和防火墙、入侵检测、病毒查杀维护等子系统，此时教育数据存储在系统运营方自有平台上，因此存储时，数据一般不会加密。当教育信息系统没有充足资源时(如广大中小学和小型的在线学习平台)，一般使用大型第三方的云存储服务，云服务提供商会提供防火墙、入侵检测、病毒查杀等服务。此时，由于数据脱离了教育信息系统主管方控制，数据内容有泄露

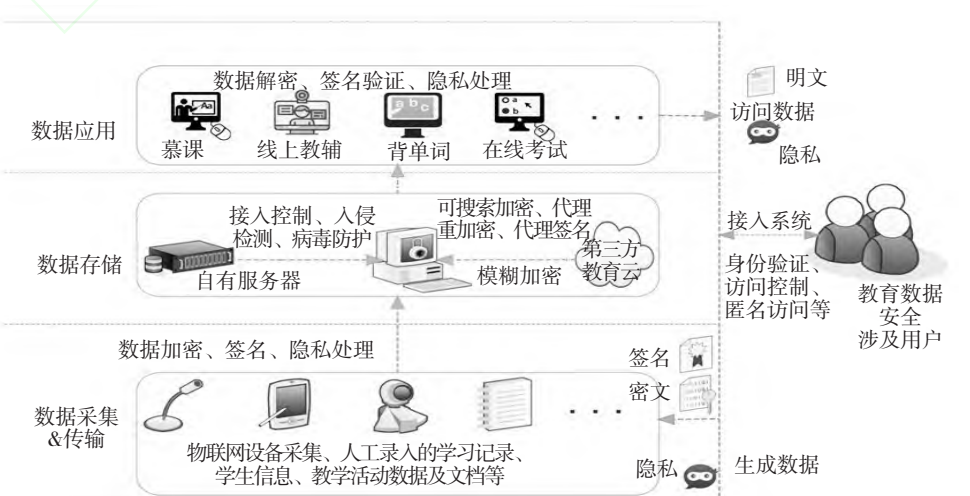

图3 教育数据安全与隐私保护框架

和被篡改风险，需要对数据进行对称加密，并生成哈希摘要后签名。系统主管方只需要用一台小型的安全设备做好加解密密钥、签名数据的存储及管理，而这台设备只对系统运维人员开放。

在教育数据使用安全保障中，需要根据业务的类型和运行机制，来决定使用一种或者几种信息安全技术的组合，构建安全的数据使用方案。数据的使用有两种类型，一种是用户去信息系统查询，如学生查询自己课程考试成绩。另一种是系统主动对外公开，如学生考试成绩的及格人数、最高分、最低分、平均分等统计信息。对于前一种数据的使用，在系统宏观层面设置身份认证机制，用户在进入业务系统时，需要输入密码、权限卡片、手机验证码、脸纹、指纹等验证手段中的一种或几种，进行身份验证，通过后方能进入系统。而后对具体的数据，使用访问控制技术，划定细分的访问权限。只有授权的用户拿到数据才能够解密，未授权用户，即使拿到数据，也无法获悉内容。对于后一种数据，系统在向外公开时，需要先去除身份标识符，而后添加差分隐私噪声值，再对外发布。数据的使用还需要和数据的存储方式关联。对于存储在第三方云服务平台上的数据，需要使用可搜索加密技术、代理重加密、代理签名技术对数据进行处理后存储，使得数据加密存储后，还可被用户检索及云平台协助验证有无被外界篡改。

五、信息安全技术深入教育应用的挑战

随着教育信息系统的泛在化、网络化，智能化的深入发展，教育信息系统内用户的数据安全及隐私越来越容易被破坏和泄露，信息安全技术的全面深入教育应用势在必行。然而信息安全技术不是功能性技术，而是一种防御性技术，它的引入，会给现有教育信息化系统带来一系列技术和社会问题的挑战。

(一)数据安全与隐私的防御性处理与教育信息系统使用快捷性之间的矛盾

要保障教育数据的安全与隐私，势必要在数据的采集和传输、处理及使用时，使用加密、签名等技术，对数据进行一系列的加、解密和签名计算、验证等安全处理。一方面在教育信息系统内部，数据的安全处理流程，会增加数据流转过程中的时间，也就相应地增加了用户使用系统的等待时间；另一方面，在教育信息系统外部，用户想要接入系统访问和编辑各类数据，需要掌握包括系统口令、身份认证、权限验证等各类安全防护操作知识与技巧，需要耗费大量的时间和分散使用精力。因而，数据的安全与隐私保障机制，会给系统用户带来诸多的不快捷。

然而，教育信息系统的建设初衷是为包括教、管人员和学生在内的教育用户，在日常的教与学相关活动中，提供信息化辅助，减少教育用户在与教与学无关的程序性事务上的时间和精力消耗，提高教与学的效率。因此，系统使用的快捷性是教育信息系统一个核心要求。

总而言之，数据安全与隐私的处理需要耗费时间、安全机制的学习和使用需要耗费和分散精力，这就与教育信息系统服务教与学、提高教与学效率、方便教育用户的建设初衷之间，形成了难以调和的结构性矛盾。不安全的教育信息系统无人敢用，不便捷的教育信息系统无人愿用，如何有效化解这种矛盾，对信息安全技术能否深入教育应用提出了一个挑战。

(二)数据安全与隐私的封闭性要求与教育数据开放共享性之间的矛盾

要保障教育数据的安全与隐私，势必要使用访问控制、权限控制、接入控制等技术，尽可能减少外界对数据的访问频率、频次和渠道，并让数据在尽可能小的范围内流通。数据的访问频率越高、频次越大，数据因有意或者无意暴露的可能性越大；访问的渠道越多，如既可以在教育系统内网访问，又可以在公网访问，因某一条渠道出现问题，造成整个系统不安全的可能性越大。数据的流通范围越大，混杂的各类用户越多，越难以监控管理，如学生基本信息是只有班主任可见，比相关班级全体老师可见要安全，本校老师可见比外校老师可见安全。

然而，一方面，教育信息化2.0的核心特点便是借助大数据分析和处理、人工智能等等新兴技术，开展学习分析、深度学习、协同学习、个性化推荐和学习评测等智慧学习研究与应用[34]。这些研究与应用得以开展的必要条件是获取和利用海量的教育用户数据，以尽可能准确地得出教育用户的状态和特征，而这种数据访问需求的频率、频次、角度和范围都是难以确定的，因此需要有自由的数据访问权限。另一方面，现实中教育资源的不均衡、不合理分布，又需要让每一个受教育者，能够获取同等的教育资源，也即每一个受教育者都应该有平等权利访问国家资源建设的任一教育信息系统数据。

总之，数据的安全与隐私需要尽可能对数据进行封闭性处理，减少与外界的联系，并缩减与外界的接触面。而教育信息化2.0对教育信息系统的智能化发展要求，又需要消除数据访问边界和障碍，教育的公平性甚至要求对教育数据进行主动开放。这当中的矛盾是散播面大、不封闭的教育信息系统不敢用，不开放的教育信息系统又不能使用。如何

有效解决这种安全与隐私要求上的封闭性和应用功能乃至社会发展的开放性要求之间的冲突，是信息安全技术深入教育应用的又一挑战。

(三)数据安全与隐私的匿名性要求与教育数据社会公信力之间的矛盾

要保障数据的安全与隐私，势必要使用数据隐私保护技术，尽可能少地对外披露数据的内容，公开较为模糊甚至某种程度上的假数据。一方面，在教育信息系统中，数据往往是复合且相互关联的，如学生的成绩数据中会蕴含基本学籍信息，班级成绩表中含有全班同学的成绩数据。在系统对外披露这些数据时，需要尽可能少地披露数据内容，如学生只能查询到自己的成绩，对外发布的成绩数据不应包含学生学号和姓名信息，这时往往会去掉学生姓名或掩盖部分学号，或者用一个只有学生本人知道的代号，这种公开模糊数据或者假数据的目的是尽可能增强数据的匿名性。另一方面，许多情况下，用户并不希望被他人知道自己访问了哪些内容，做了哪些事务，如在教学评价和同伴互评的应用中，这些数据的公开，往往会对用户造成不利影响。

然而，教育公平性对教育数据有着严格的真实性与公正性要求，真实性要求对数据不能进行修改，公正性要求对数据不能隐瞒，即所有相关数据必须完全公开，并能够被用来确认教育用户本人和他人信息。这种真实性和公正性在事关教育用户核心利益的事项中(如学生成绩、考生成绩、电子投票结果的发布)，直接关乎教育数据主管机构的社会公信力，轻则引发用户间的不满，重则导致社会群体事件。

总之，数据安全与隐私需要尽可能地减少对数据内容和用户身份的披露，以提高数据的匿名性，而教育数据的社会公信力，又要求使用更多与数据内容关联性不大的数据信息来确保数据的真实性和公正性。这两者带来的冲突是不匿名的数据泄露用户隐私、无人敢用，而不完全公开的数据经不起检验、没有社会公信力，没有使用价值。如何解决这种数据匿名性和公信力之间的冲突，是信息安全技术深入教育应用的又一挑战。

六、结论与建议

教育信息化的发展已经进入深水期，教育数据安全与隐私已经引起了各方注意，且信息安全技术自身已经有一定发展。但在信息安全技术深度融入教育应用的目标和当前并不理想的研究及应用现状间，横亘着一系列技术和社会问题的挑战需要面对。面对如此纷杂的应用挑战，本研究对未来信息安全技术深入教育应用做出如下展望。

(一)信息安全技术的使用权和决定权分离

在教育信息系统中应用信息安全技术，为避免对用户正常的使用过程造成干扰，带来不便性，应当将信息安全技术的使用权和决定权分离。也即是说，在信息安全技术保障教育数据安全与隐私过程中，系统使用了哪些信息安全技术，怎样使用这些安全技术，用户并不用关心，用户所需要关心的是决定是否使用系统推荐的安全技术来解决数据会面临哪些风险。因为用户使用教育信息系统主要是用来完成功能性需求，而不是安全技术的防御性需求。而面临哪些安全风险，应该采取哪些安全措施，则应由教育信息系统提供并且承担责任。一旦用户决定使用安全措施，则所有的安全相关处理应尽可能在后台处理，使用诸如人脸、红外乃至基于大数据统计分析的信息安全技术，进行相关安全性处理，尽可能减少用户刻意的参与，而一旦用户的参与不可避免，则应当使用图形可视化、乃至智能语音提示交互式的操作进行。总之，技术归系统，决定在用户，如此，可有效降低信息安全技术使用对用户造成的不便捷干扰，提高用户的使用意愿。

(二)数据安全共享的权责利对等原则

在教育信息系统中，用户之所以使用信息安全技术对数据进行封闭化管理与使用，不愿意将数据对外开放共享，主要是基于对数据使用的权责利不清晰的担忧，因此，有必要对此进行明确。用户对数据共享具体的担忧，一方面是自己付出了大量精力和资源建设的数据内容，一旦对外公布，有可能引发产权纠纷，在没有明确的产权收益前，不愿意对外开放。对此，要做的是建立和完善教育数据知识产权认定机制，充分尊重数据建设者对此数据的所有权，并在此技术上使用数字签名或数字水印技术加以保证；二是共享出去的数据内容被人泄露、剽窃、或用于盈利。对此，需要明确谁使用，谁分享收益，谁泄密，谁负责的权责利对等原则，并使用可追踪来源的数字水印技术，对不同的渠道和个体施加不同的信息安全标记，将数据从一开始的无序开放到遇到安全问题的完全关闭到明确权责利的有序开放。

(三)数据匿名性与公正性独立第三方认证

在教育信息系统中，对于事关用户核心权益的教育数据，如考试、考评成绩数据，应当推行独立第三方认证并发布的机制。教育信息系统之所以要对数据进行匿名化处理，主要目的是为了保护用户隐私。然而，用户隐私泄露危害短期内并不会立刻出现，但在成绩数据带来的直接短期收益下，用

户却希望公开所有原始数据。这当中的问题在于教育数据管理者，既是数据的生成、处理者，又是数据的监督者。这种监督与被监督角色集于一身，既难以确保自身不出现问题，也难以对外令人信服。而推行独立第三方认证，对教育数据管理者对数据的采集、匿名化处理进行全过程监督，而最终将签名的匿名化数据交由第三方发布。如此这般，将数据真实性和公正性的监督角色交由与教育数据利益无关的独立第三方来确保，就避免了数据管理者自身内部出问题以及匿名化数据的真实性问题。相应地，外界对于数据的公正性也就有了基本的信任基础，而数据的匿名性同时也得到了保证。

概述之，“中国教育现代化2035”这一教育现代化阶段性工作能否稳步推进，教育数据安全是其中一项不可或缺的因素。站在历史发展的角度，第三次工业革命是信息传递途径的革命，正在爆发的第四次工业革命是数据消化吸收方式革命。在这场浩浩荡荡的世界变革大势中，教育是确保中华民族立于世界民族之林的根本基石，教育信息化是构筑这一基石的良工利器，而教育数据安全与隐私保护是防止这一良工利器反噬的必要护具。相信教育数据以及学习者隐私在信息安全技术的保驾护航下，教育现代化一定能够稳步健康发展。

参考文献：

[1] 梁林梅,赵柯杉.美国K-12在线教育:现状、系统结构与政策分析[J].中国电化教育,2017,(11):65-71.
[2] David B.Whittier,周梦雅.网络伦理教育与网络心理[J].中国电化教育,2012,(3):1-7.
[3] 李青,李莹莹.大数据时代学习者隐私保护问题及策略[J].中国远程教育,2018,(1):29-36.
[4] 杨现民,赵鑫硕等.网络学习空间的发展:内涵、阶段与建议[J].中国电化教育,2016,(4):30-36.
[5] 杨现民,唐斯斯等.发展教育大数据:内涵、价值和挑战[J].现代远程教育研究,2016,(1):50-61.
[6] Pardo A,Siemens G.Ethical and privacy principles for learning analytics[J].British Journal of Educational Technology,2014,45(3):438-450.
[7] 徐鹏,王以宁等.大数据视角分析学习变革——美国《通过教育数据挖掘和学习分析促进教与学》报告解读及启示[J].远程教育杂志,2013,31(6):11-17.
[8] Rubel A,Jones K M L.Student privacy in learning analytics:An information ethics perspective[J].Information Society,2016,32(2):143-159.
[9][15] 李青,张鑫.区块链:以技术推动教育的开放和公信[J].远程教育杂志,2017,35(1):36-44.
[10] Blakley B,Mcdermott E.Information security is information risk management[A].Proceedings of the 2001 Workshop on New Security Paradigms[C].Cloudcroft,New Mexico:ACM,2001.97-104.
[11] 张焕国,杜瑞颖等.信息安全:一门独立的学科,一门新兴的学科[J].信息安全与通信保密,2014,(5):37-39.
[12] 嵇波.基于安全云服务的开放课程应用研究[J].江苏教育研究,2015,(18):46-50.
[13] 李以斌,牟大伟.教育云平台的敏感信息保护技术研究[J].网络空间安全,2016,7(11):102-106.
[14] 赵慧琼,姜强等.大数据学习分析的安全与隐私保护研究[J].现代教育技术,2016,26(3):5-11.
[16] 俞海燕.安全高效的跨高校档案信息共享系统[J].现代教育技术,2010,20(S1):126-129.
[17] 李凤英.代理签名技术在远程教育中的应用模型及实现研究[D].上海:华东师范大学,2011.
[18] Greschbach B,Rodríguez-Cano G,et al.Design of a Privacy-Preserving Document Submission and Grading System[A].Proceedings of 20th Nordic Conference[C],Stockholm,Sweden:Springer,2015,64-71.
[19] 李凤银.远程教育管理系统的身份认证研究与实现[J].电化教育研究,2004,(9):49-52.
[20] 王金富.远程教育环境中的安全性分析与实现[D].上海:华东师范大学,2007.
[21] 李凤英,薛庆水等.基于认证的移动学习私密保护模型和方案[J].现代远程教育研究,2013,(3):72-77.
[22] 李凤英,何屹峰等.MOOC学习者身份认证模式的研究——基于双因子模糊认证和区块链技术[J].远程教育杂志,2017,35(4):49-57.
[23] 王云,史浩山等.一种基于PKI安全的现代远程教育系统[J].中国电化教育,2004,(10):82-84.
[24] Klobucar T,Senicar V,et al.Privacy and personalisation in a smart space for learning[J].International Journal of Continuing Engineering Education and Life-Long Learning,2004,14(4/5):388-401.
[25] Anwar M,Greer J.Facilitating Trust in Privacy-Preserving E-Learning Environments[J].IEEE Transactions on Learning Technologies,2012,5(1):62-73.
[26] 李凤英,齐宇歆等.大数据视域下的虚拟学习社区安全研究——基于门限代理签名的协同学习系统探讨[J].远程教育杂志,2013,31(4):76-82.
[27] Obiria P B,Kimwele M W.A location-based privacy-preserving m-learning model to enhance distance education in Kenya[J].Journal of Computers in Education,2017,4(2):1-23.
[28] 胡世清,程国雄.基于Silverlight防舞弊计算机网络考试系统的研究和实现[J].电化教育研究,2010,(12):47-51.
[29] Atoum Y,Chen L,et al.Automated Online Exam Proctoring[J].IEEE Transactions on Multimedia,2017,19(7):1609-1624.
[30] 郑炜冬.铸造高校网络考试的公平之盾——综合防舞弊网络考试系统设计与实现[J].现代教育技术,2012,22(5):102-107.
[31] Kaiiali M,Ozkaya A,et al.Designing a Secure Exam Management System (SEMS) for M-Learning Environments[J].IEEE Transactions on Learning Technologies,2016,9(3):258-271.
[32] 夏大飞.高考数据隐私保护技术的应用研究[D].重庆:西南大学,2013.
[33] Gursoy M E,Inan A,et al.Privacy-preserving learning analytics: Challenges and techniques[J].IEEE Transactions on Learning technologies,2017,10(1):68-81.
[34] 任友群,冯仰存等.融合创新,智能引领,迎接教育信息化新时代[J].中国电化教育,2018,(1):7-14.

作者简介：

刘梦君：讲师，博士，研究方向为教育数据安全挖

掘、个性化学习安全推荐(lmj_whu@163.com)。

姜雨薇：在读本科生，研究方向为教育数据挖掘(jiang_yw1201@163.com)。

曹树真：副教授，博士，研究方向为教育原理和教育伦理(602945600@qq.com)。

杨兵：教授，博士，研究方向为智慧学习、自适应学习系统(yangbing@126.com)。

Analysis of the Applications of Information Security Technology in Educational Data Security and Privacy

Liu Mengjun[1], Jiang Yuwei[1], Cao Shuzhen[1], Yang Bing[2]

(1.Hubei University, Faculty of education technology, Wuhan Hubei 430062; 2.Hubei University, Smart learning research center, Wuhan Hubei 430062)

Abstract: Nowadays, properly using information security technology to protect education users' data security and personal privacy in cyber space, is of great importance to the national cyber-security, as well as to the education users' human rights. This paper starts with analysis of the security technology architecture under the perspective of education, and then discriminates the relationship between education security and education data security, gives the theoretical connotation of education data security and privacy. Through comprehensive literature review, we conclude the state-of-art research on education data security and privacy, and then give the security and privacy goals of education data security and privacy, and show the common process of information security technology. Finally, we point out the challenges faced in education data security and privacy-preserving, and discuss its future work.

Keywords: Education Informationization; Secure Education Information System; Education Data Security and Privacy; Learning Security and Privacy

收稿日期：2019年1月10日

责任编辑：邢西深

(上接第113页)

A Research on Criteria for Identifying Teaching Quality of Open Online Courses in Universities Based on Quality Function Deployment(QFD)

—Needs Analysis of the Value Subjects

Yang Xiaohong[1], Hao Zhao[1], Zhou Haijun[1], Zhou Xiaozhang[2], Li Yunfu[3]

(1.College of Educational Technology, Northwest Normal University, Lanzhou Gansu 730070；2.College of Educational Science, Zhoukou Normal University, Zhoukou Henan 466001；3.College of Educational Science, Shaanxi Xueqian Normal University, Xi'an Shaanxi 710061)

Abstract: Acquiring the needs of value subjects is the first step in research on criteria for identifying teaching quality of open online courses in universities. The present paper collects the source materials of the value subjects' needs of open online courses through literature review, text analysis of learners' evaluation, questionnaire survey and interviews. According to the KJ method, the hierarchical needs list of value subjects is obtained by extracting keywords from the source materials, clustering, de-duplication, grouping, refinement and summarization. And the weight value of each needs item is determined by expert-assessment method and analytic hierarchy process. This research lays the foundation for the applying of quality function deployment (QFD) technology, helping diversified value subjects' needs transform into teaching characteristics of course and forming criteria for teaching quality and criteria for its identification.

Keywords: Open Online Course; Needs of Value Subjects; KJ Method; Analytic Hierarchy Process

收稿日期：2019年3月21日

责任编辑：赵云建