文章编号：2095-2163(2021)03-0121-03 中图分类号：TP309 文献标志码：A

新媒体时代网络犯罪下的云取证技术研究

李玲俐
（广东司法警官职业学院，广州 510520）

摘 要：利用计算机和新媒体技术，网络犯罪案件则呈现出一些新的特征，云计算平台是网络攻击的最大目标。针对新媒体环境下云平台的安全隐患，以及传统电子取证的局限性，阐述云取证工作发展的迫切性，探讨了网络犯罪下云取证的研究热点及模型，以及现有工作所面临的各种挑战，并提出云取证领域今后的改进措施和研究方向。

关键词：新媒体；网络犯罪；云取证；云计算；电子取证

Research on cloud forensics technology under network crime in New Media Era

LI Lingli
（Guangdong Justice Police Vocational College，Guangzhou 510520，China）

【Abstract】 With the use of computers and new media technologies，cyber－crime embodies some new features，and cloud computing platforms are the biggest targets of Internet attacks. In view of the hidden security risks of cloud platform under the new media environment and the limitations of traditional electronic forensics，this paper expounds the urgency of the development of cloud forensics，discusses the research hotspots and models of cloud forensics of network crimes，as well as various challenges faced by the existing work，and proposes the improvement measures and research directions in the field of cloud forensics in the future.

【Key words】 new media；cyber-crime；cloud forensics；cloud computing；electronic forensics

0 引 言

相对于传统媒体，新媒体是一种以数字压缩、无线网络和移动通信技术进行信息传播的媒体新形态，通过网络电视、视频、博客、电子杂志等互联网、无线通信网、卫星等渠道，电脑、手机、数字电视等终端，以及公交、地铁、航空电视和大型 LED 屏等户外新媒体，向用户提供信息、传播服务。其实时性、交互性、大容量，以及受众选择性不断增多、表现形式多样使之能跨越地域、行政范围、打破各媒介之间的阻碍而实现全球化传播[1]。

新媒体时代网络和信息技术快速更新，云计算、大数据、物联网、人工智能等应用广泛的同时，互联网和云环境成为网络犯罪的平台。本文分析新媒体时代网络犯罪的现状和特征，提出云环境安全隐患下，云取证相对传统电子取证的优越之处，详细介绍网络犯罪下云取证技术的研究模型，阐述了云取证所面临的挑战，最后提出云取证技术未来的研究方向。

1 网络犯罪下云环境的安全问题和云取证的提出

1.1 网络犯罪的现状

网络犯罪是指行为人借助工具或以网络资产为对象，运用计算机技术、网络知识，以及编程、加解密技术对系统或信息进行犯罪攻击，或利用软件指令实施犯罪[2]。许多有害信息会通过网络传播，病毒、木马、钓鱼攻击、网络诈骗比例在一定时期内也表现出上升倾向，严重威胁互联网经济安全，分工明确的灰色产业链数量和比例在悄然增大，跨国网络犯罪的可能性有所增加，犯案方式也呈产业化和多元化，成本低、传播快、隐蔽性高、智能化、低龄化特征越来越显著，对社会各个领域带来巨大的影响和危害。

1.2 云计算平台及其安全隐患

云计算是将存储在计算机、移动电话和其它设备上的数据信息集中协调工作，使用者只需投入较少的开销，便能随时联网随时获取云端资源，包括各种计算产品、数据存储空间和大量的云数据等。云计算具有大规模、资源虚拟化、高分布性、高可靠性、资源池共享、快捷低廉等优点，为企业和用户提供了便利，越来越多的人习惯将自己学习、工作和生活有关的电子数据存储在云端，这些电子资源也包括了大量的隐私信息和商业秘密数据[3]。

云计算平台飞速发展的同时，其安全面临着巨大的威胁，许多借助云服务的案例，如：黑客传播恶

基金项目：2020 年度广东省司法行政研究课题（GDSF20070）。
作者简介：李玲俐（1977-），女，硕士，教授，主要研究方向：数据挖掘、模式识别、网络安全。
收稿日期：2020-11-30

意程序、用户数据被破坏或泄露、各种持续性威胁攻击、非法数据存储等[4]。虽然云平台自身设置了多道的安全防线,但网络犯罪分子技术和手段越来越智能,通过蓄意攻击或破坏云服务节点,企图入侵内部破坏或窃取有价值的信息,其犯罪痕迹往往只在云端或网络才有记录[3];云计算平台的特性使得传递信息又快又方便,犯罪成本低,有些犯罪分子利用法律漏洞实施钓鱼等行为。目前各云端数据越来越多,云平台成为网络攻击的重灾区,其安全隐患令人堪忧,取证工作变得越来越迫切。

2 网络犯罪下的云取证技术

2.1 云取证的提出

云计算和大数据环境下,电子数据存在海量性、动态性、资源共享性、分散存储性、数据易失性和易篡改性等特点,传统的电子取证有些是单机取证,有些是网络集群下的简单取证[3],但在新媒体时代的云计算平台下,电子数据具备传统电子证据的一般特性,且动态性更高,带有时间戳功能;取证工具必须分工细致,尽量在隔离环境下使用,在很大程度上限制了取证工作的开展。传统的电子取证无论是取证框架、取证方式还是取证工具都已经不能适用于当前云环境下的取证问题,而且,云取证的过程也比传统电子取证所涉及的对象更多、交互更复杂[5]。

云取证是云计算技术和传统的电子取证的交叉学科,是云安全的重要组成部分[6],是电子取证中一个新兴热门的研究领域[4]。云取证工作是针对云犯罪收集数字取证数据的过程[7],能够发现云平台漏洞和各种攻击特征或类型,通过调查、匹配和分析云安全攻击行为[8],采集犯罪行为的有关证据,对网络犯罪分子进行打击、威慑和追责,维护和促进云平台系统的稳定发展[4]。

2.2 网络犯罪下云取证思路和模型的研究

云取证模型采用通用的取证框架,集合一些规范的取证方法和取证流程,符合未来的新型电子取证的各项需求[9],增强获取电子证据的自主性和智能性,提高电子证据的安全性能以及取证的效率[10],对电子取证的调查、操作和研究起着引导作用[9]。

目前,越来越多的研究人员对网络犯罪下的云取证工作有了清晰的思路和可行的取证模型研究。杨淑棉等人[11]针对云计算环境下的犯罪证据完整可靠性问题,提出了 IaaS 模式下实时云监控取证系统的思路和方法。高元照[4]结合云平台下的取证场景,提出了一种持续性取证模型。王健等人[12]提出一种能改变电子证据的静态属性,并支持精准语义的取证模型。新媒体时代,犯罪分子散布虚假消息,金骁[13]研究了解决图像视频操作的 4 个问题,可以更准确鉴别海量的多媒体信息的真假。徐蕾[14]提出一种区块链技术的可验证、不可篡改的取证系统,李维奉等人[8]提出了一个面向云计算平台的隐私侵犯的追踪取证系统。

2.3 云取证面临的挑战

证据是对犯罪分子是否进行判决的主要依据,针对云犯罪的取证工作,法律方面包括司法管辖、用户隐私权保护和数据完整性问题;技术方面存在大规模的异构数据的混合[14]存储等问题。无论是法律法规、还是技术标准体系都为传统电子取证工作带来极大的挑战[3]。对此拟展开研究分述如下。

2.3.1 云取证相关的法律法规不够完善

(1)司法权管辖问题。云计算平台具有资源虚拟化和分布式存储等特点,同一用户可使用不同云端资源,不同的云服务器可能分布在不同的区域,甚至在国外,各地的法律法规不同,取证流程和标准也不同,数据定位和提取困难使得境外取证成为难题[5]。

(2)用户隐私权问题。云计算平台下,用户的各种数据和信息存储在云端,由云服务提供商统一管理,资源的所有权、使用权和管理权分离,数据隐私很容易被泄露,取证人员很难从用户层面实行网络取证。另外,不同用户可共享同一云服务器资源。专业人员进行云犯罪取证时,通常会触碰到其他无关用户的信息安全[7],也会涉及并威胁到一些个人隐私或者商业机密的情况。这种复杂性问题在国内现行的法律法规中还有待完善,特别是对公民隐私权的保护上也仍存在隐忧,取证人员面对上述问题时常无法很好把握力度[5]。

(3)数据完整性问题。云计算环境中,电子数据保存在哪个设备、哪个节点是不确定的,很难通过日志分析或者数据拦截等方式取得数据。因此在进行云犯罪取证的时候,如何保证电子数据的完整性一直是一个聚焦讨论并亟待解决的问题[5]。

2.3.2 主流的云取证技术标准和体系不够成熟[8]

(1)电子数据规模大,异构数据的混合存储。随着电脑、平板、手机等电子产品的使用,及数量、容量的迅速增长,这些必需品生成了很多不同格式的数据,大量结构化、半结构化、非结构化的数据同时存储在云服务端,取证时会收集到大量无关或非连

续型数据,而现有的取证工具在分析各种云计算平台不同格式的数据时还存在一定的局限性[4],增大了取证和分析难度。

(2)云端数据易失性。云计算平台下电子证据的易失性主要体现在篡改和删除的数据难以恢复。比如,犯罪分子使用完数据并将其删除,云服务提供商为保护用户和数据隐私,将这些数据及相关的元数据完全删除[4]。许多电子数据在云取证前已经被篡改或删除,因此,云取证一般要求实时在线取证,但是如此一来又会为云平台带来挑战。

(3)时间戳不一致。云计算平台下,同一用户的数据有很多时候是存储在不同的时区,时间戳会受到不同的系统、不同的文件,以及各种状态、运行变化等因素的制约,甚至出现不同步的情况,极大增加了分析时间戳的复杂性[4],犯罪过程可能会被重新构建。

2.3.3　技术与法律交叉学科的云取证专业人员相对缺乏

云环境下网络犯罪分子已经具备了高科技电子设备和技术,云端数据分散存储,其共享性、动态性、易篡改、易失性等特点,使得云取证工作人员必须对这些大数据进行及时全面的分析,因而面临更专业的技术挑战。目前,国内高质量的的云取证专业人员还很缺乏。

3　结束语

云计算的各项研究已相对成熟,云取证是针对各种违法犯罪活动的取证过程,其发展相对比较晚,存在取证过程不够智能化、开销较大、专业技术人员缺乏等问题,本文分析新媒体时代网络犯罪下云环境的安全问题,阐明云取证技术作为事后追责与惩罚的法治手段之一,对打击云犯罪活动和维护云计算环境安全具有重大意义[3];论述网络犯罪下云取证思路和模型的研究,提出当前云取证在技术和法律方面面临的挑战。尽管如此,云取证也拥有更多新的机遇,其势必会在未来的云犯罪调查、用法和研究等方面有着广阔的发展前景,主要体现在如下方面。

(1)除了在技术上构建更加完善的云取证模型,快速识别云犯罪行为,也将结合具体的司法实践问题,深入分析其中涉及到的法律法规事项,进而规范和细化、且找出各种应对策略[3],保证取得的电子证据能合法使用。

(2)技术和法律两个方面相互协同,用技术推进法律法规的改进,用法律法规保障技术和标准的施行。

(3)云取证分析算法的优化,使得取证费用降低和准确度提升,云平台的安全问题也将得到进一步改善。

参考文献

[1] 百度百科. 新媒体[EB/OL]. [2020-09-28]. https://baike.baidu.com/item/新媒体/6206?fr=aladdin.

[2] 网络犯罪_百度百科[EB/OL]. [2020-09-28]. https://baike.baidu.com/item/网络犯罪/10142346?fr=aladdin

[3] 李翠. 云计算环境下电子数据取证研究[D]. 重庆:重庆邮电大学, 2018.

[4] 高元照. 云计算取证模型及其关键技术研究[D]. 郑州:解放军信息工程大学, 2017.

[5] 高运,伏晓,骆斌. 云取证综述[J]. 计算机应用研究, 2016,33(1):1-6.

[6] RUAN K, CARTHY J, KECHADI T, et al. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results[J]. Digital Investigation, 2013, 10(1): 34-43.

[7]丁丽萍. 云环境下的电子数据取证技术研究[J]. 中国信息安全, 2019(5):59-60.

[8] 李维奉,羌卫中,李伟明,等. 云环境隐私侵犯取证研究[J]. 网络与信息安全学报, 2018,4(1):26-35.

[9] SHRIVASTAVA A K, PAYAL N, RASTOGI A, et al. Digital forensic investigation development model [C] //2013 5th International Conference on Computational Intelligence and Communication Networks(CICN). Mathura, India: IEEE, 2013: 532-535.

[10]公伟, 刘培玉, 迟学芝,等. 云取证模型的构建与分析[J]. 计算机工程, 2012(11):14-16.

[11]杨淑棉, 王连海, 张淑慧,等. 一种 IaaS 模式下的实时监控取证方法[J]. 山东大学学报(理学版), 2017,52(6):84-91.

[12]王健,唐振民. 面向领域特征的云取证模型[J]. 南京理工大学学报(自然科学版), 2016,40(4):477-484.

[13]金骁. 数字多媒体被动取证关键技术研究[D]. 天津:天津大学, 2018.

[14]徐蕾. 基于区块链的云取证系统研究与实现[D]. 绵阳:西南科技大学, 2014.