轻量级安全隔离的虚实互联平台设计与实现*

贾星威，田晓娜，张宏斌，刘楚涵，石春竹，崔　轲
（华北计算机系统工程研究所，北京　100083）

摘　要：通过对虚实互联平台的现状研究，针对现有平台在安全性、实用性、灵活性等方面的不足，提出了一种轻量级安全隔离的虚实互联平台设计方法。首先对轻量级安全隔离的虚实互联平台进行理论性的实现研究，提出实现方法；然后在现有实验环境基础上，结合理论实现途径给出实际的平台搭建及部署设计，进行了平台的实现；最后针对搭建完成的平台进行了能力验证与应用。实验结果表明所提出的轻量级安全隔离的虚实互联平台具有良好的实用性，与现有方法相比具有一定的优势。

关键词：虚实互联；轻量级；安全隔离；云平台
中图分类号：TP393　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2023. 06. 009
引用格式：贾星威，田晓娜，张宏斌，等. 轻量级安全隔离的虚实互联平台设计与实现［J］. 网络安全与数据治理，2023，42(6)：54 - 59.

Design and implementation of virtual-real interconnection platform with lightweight security isolation

Jia Xingwei，Tian Xiaona，Zhang Hongbin，Liu Chuhan，Shi Chunzhu，Cui Ke
（National Computer System Engineering Research Institute of China，Beijing 100083，China）

Abstract：Based on the research of the status quo of virtual-real interconnection platform，this paper proposes a lightweight security isolation design method for virtual-real interconnection platform in view of the shortcomings of existing platforms in security，practicability，flexibility and other aspects. Firstly，the theoretical implementation of lightweight security isolation virtual-real interconnection platform is studied，and the implementation method is proposed. Then on the basis of the existing experimental environment，combined with the theoretical approach，this paper gives the actual platform construction and deployment design，and completes the realization of the platform. Finally，the capability verification and application of the completed platform are carried out. The experimental results show that the lightweight security isolation virtual-real interconnection platform proposed in this paper has good practicability，and has certain advantages compared with the existing methods.

Key words：virtual-real interconnection；lightweight；security isolation；cloud platform

0　引言

随着网络仿真、云计算技术的发展，对虚实互联技术的需求也日益增加。通过对虚实互联技术的研究能够有效提高实际场景模拟仿真构建任务的逼真还原程度，具有较强的现实意义[1]。

然而目前对于虚实互联平台的研究并不完善，平台在安全性、实用性、灵活性等方面仍有不足。本文围绕虚实互联网平台展开研究，提出一种轻量级安全隔离的虚实互联平台的理论设计方案，同时结合客观实验条件给出了实际平台的部署搭建方法并进行了能力验证。

*基金项目：国防基础科研计划（JCKY2020211B005）

1　虚实互联平台研究现状

虚实互联平台能够在统一的操作体系和运行环境中对实物资源和虚拟资源进行管理，其通用架构可以抽象为支撑层、平台层及应用层，其中支撑层为平台提供资源支撑，包括通用资源（如服务器、交换机）及异构资源；平台层提供虚拟资源及实物资源管理的功能支撑，包括虚拟化、实物接入、网络映射、虚拟网络管理及资源建模等功能；应用层为虚实互联平台的核心功能层，包括对虚实资源统一管理的网络拓扑及资源管理。虚实互联平台基本架构如图1所示。

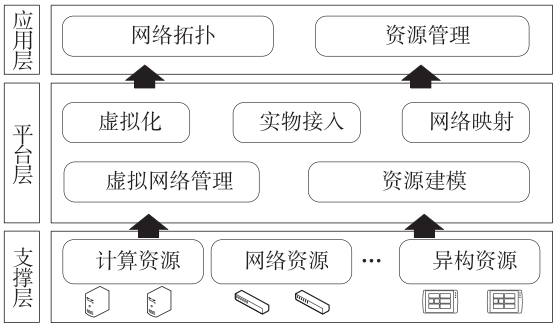


图 1　虚实互联平台基本架构

现有的虚实互联平台种类较多，实现方式也是多种多样，本文选取其中三种具有代表性的实现方式进行介绍对比。

方法一：使用云框架与专用硬件（如 SDN 交换机），通过对流量进行标记、控制、转发，从而以导流的方式实现虚实互联[2]。

方法二：使用 Mininet 的虚拟网络与 OpenStack 的虚拟网络规模乘性叠加实现大规模虚实互联仿真网络的快速构建[3]。

方法三：通过对实物设备数字建模，将实物设备的实际网络连接关系映射到虚拟网络拓扑，从而实现虚实资源的统一管理[4]。

上述方式仍有其固有的弊端：方法一对于专用设备的依赖性强，且安全性差；方法二主要进行理论性大规模网络节点的构建，在实际工作中的实用性不强；方法三的开发工作量大，且网络的灵活性差，构建的网络较为固定。针对这些问题，同时考虑到平台应具备灵活、实用、安全、易拓展、轻量等特性，本文对虚实互联平台理论展开研究，旨在提出一种轻量级安全隔离的虚实互联平台。

2　轻量级安全隔离的虚实互联平台理论研究

针对现有虚实互联平台存在的问题，本文提出一种轻量级安全隔离的虚实互联平台的实现方法，如图 2 所示。该方法主要在基础框架部署、安全隔离、轻量化及虚实网络互联方面给出设计方案，从而解决现有平台存在的问题。

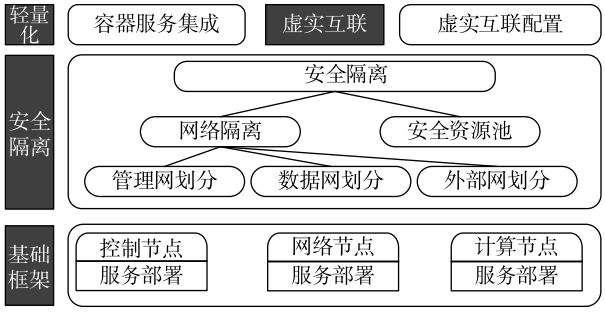


图 2　轻量级安全隔离的虚实互联平台架构

基础框架设计主要依靠现有云架构的支持，部署虚拟化、资源管理、网络管理及身份权限管理等功能，为平台提供基础的功能支撑。通过基础框架，可以实现虚拟节点、网络、子网、端口、路由器、固定 IP、浮动 IP、外部网络、项目网络及安全组等资源的模拟，从而进行虚拟网络[5]的构建。基础框架可以直接对网络、子网、端口三类核心资源进行操作，支持以 API 的方式管理 L3 路由器、防火墙、负载均衡器、虚拟专用网络，从而实现 L3 ~ L7 层的网络服务。

安全隔离主要依靠应用网络安全隔离技术及建立安全资源池实现。网络安全隔离为用户及物理资源提供一个逻辑隔离的广播域，可以按照隔离需求进行子网的划分，能够对网管、DNS 进行配置，并能够进行 IPv4/v6 的 CIDR 地址池的管理。云安全资源池通过对 IPS、防火墙、日志审计等安全资源建立镜像实现，依靠安全资源池可以为平台的虚拟网络与实物网络提供安全支撑。

轻量化主要依靠容器技术实现。现有平台虚拟节点创建大都依靠 CPU 虚拟化技术，节点创建受 CPU 数目的影响，较为冗余，灵活性不强。依靠容器技术[6]进行节点创建是进程级别的轻量化创建，可以极大程度地提高平台虚拟节点的创建数量，从而提高平台的灵活性和可拓展性。

虚实网络互联主要依靠 Open vSwitch 实现，通过创建虚拟路由器、交换机，根据拓扑逻辑关系配置虚拟网络的连接，从而实现网络拓扑的逻辑映射。绑定虚拟交换机到物理网卡，通过对地址资源池的管理，为虚拟节点分配并绑定浮动 IP，可以实现虚拟节点与实物节点间的互联互通，从而实现虚拟网络与实物网络的连接。

3　轻量级安全隔离的虚实互联平台设计

本节主要结合实际硬件环境，在理论研究基础上，给出实际的平台设计，进行轻量级安全隔离的虚实互联平台的搭建。

3.1　基本框架设计

虚实互联平台搭建可以将全部组件部署在同一台服务器上从而构建 all-in-one 的平台环境，也可以通过将不同组件部署在不同服务器上从而构建分布式的平台环境[7]。相对来说 all-in-one 的平台环境占用资源较少但不利于管理维护，而分布式的平台环境便于维护管理和大规模拓展但需要占用较多硬件资源支撑，不同部署方式各有优劣，需要根据实际情况进行选择。本文结合实际情况，采用第二种部署方式进行平台环境搭建，硬件设备使用三台服务器和一台交换机，其中一台服务器作为控制节点（Controller），一台服务器作为网络节点（Neu-

tron)，一台服务器作为计算节点（Compute），交换机作为这三台服务器之间的连接，其他需要接入的设备也可以通过该交换机接入。

采用分布式部署需要在不同节点上安装其所需的组件及服务，控制节点、网络节点、计算节点部分组件部署关系如图 3 所示。

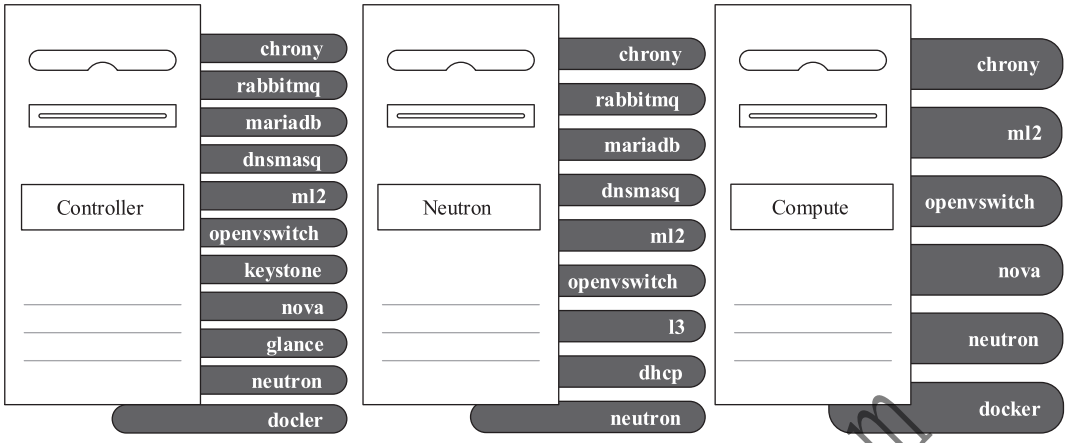


图 3　部分组件部署关系

其中，控制节点主要负责对其他节点的总体控制，包括网络的创建分配、虚拟机的创建/修改/删除、存储的管理分配等，同时在控制节点上部署了认证服务、计算服务、镜像服务及网络服务。网络节点可以实现网络管理、网络拓扑管理功能，对平台提供网络、负载均衡、防火墙、二层交换、三层交换及 VPN 支持，同时在网络节点上部署有网络服务。计算节点负责对所有资源、认证、网络等进行管理，并可为平台提供良好的可拓展功能，同时在计算节点上部署有计算服务、网络服务。

3.2　互联互通配置方法设计

实现实物设备与虚拟网络之间的互联互通有多种配置方式[8]，本平台主要采用浮动 IP 的方式实现。在虚实互联平台中，虚拟机连接在虚拟局域网中，虚拟局域网与外部网络通过虚拟路由连接起来，可以使虚拟机访问外部网络。在网络节点中这一功能主要通过 Open vSwitch 实现[9]，通过将外部网卡与 br-ex 绑定起来，虚拟机便可以通过网桥访问到外部网络，具体实现原理如图 4 所示。

如果要使用外部网络访问虚拟机，只需使用外部网络创建浮动 IP，并将浮动 IP 绑定到虚拟机对应的网络端口即可，这一过程在网络节点中主要是通过 iptabes 使用 . Nat转发实现[10]。经过 . Nat 转发，可以将需要发送给浮动 IP 的流量都转发到端口绑定的固定 IP 上，从而使虚拟机可以接收外部网络发来的数据。

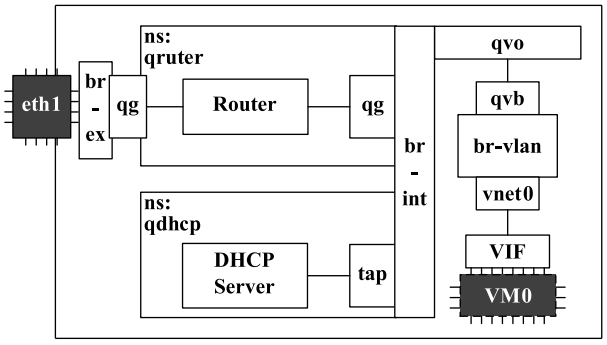


图 4　虚拟机与外部网络连接

3.3　安全隔离方法设计

安全隔离设计主要包括对网络的隔离设计与安全资源的池建立。

在三台服务器中，控制节点、计算节点的服务器需要两张网卡，分别供管理网和数据网使用，网络节点的服务器需要三张网卡，分别供管理网、数据网和外部网使用。管理网、数据网相分离，一方面可以提高平台的安全性，因为在虚拟机内虚拟机无论怎样使用都只会对数据网造成影响，不会影响到管理网，另一方面这样做可以实现流量分离，便于对数据网和外部网配置流量策略从而进行流量管理。在交换机上管理网、外部网为主干道模式，数据网为汇聚模式。逻辑网络隔离连接方式如图 5 所示。

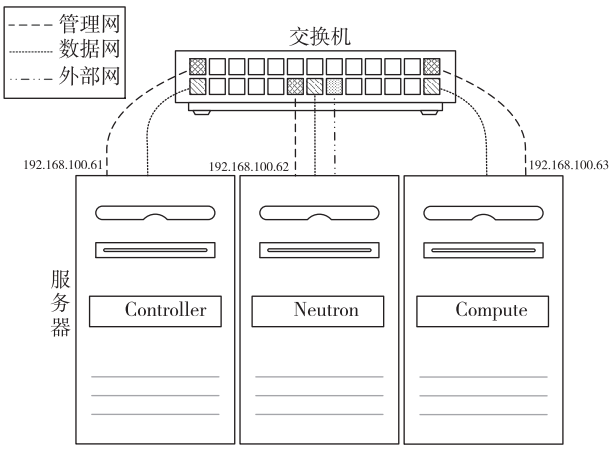


图 5　网络隔离连接

实物设备可以添加到统一的资源管理中进行维护，并通过交换机接入该虚实互联平台，如图 6 所示。

安全资源池的主要实现方式是建立安全资源镜像，通过虚拟化数据审计、虚拟化 IPS、虚拟化防火墙和虚拟化日志审计为平台提供安全资源支持，并依靠平台的资源管理功能，对安全资源进行集成与统一管理，如图 7 所示。

图 6　实物接入示意

图 7　安全资源池

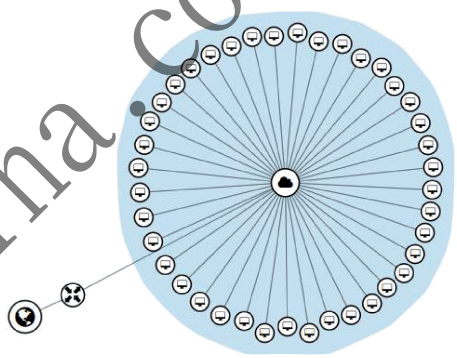


图 8　批量创建拓扑

4　平台能力验证与应用

部署完成后的虚实互联平台可用于多种虚实互联场景的构建[11]，平台可以满足不同场景需求下的复杂任务要求。本节主要对轻量级安全隔离虚实互联平台的能力进行客观统计测试，并进行实际场景构建。

4.1　平台能力验证

通常用于评价虚实互联平台能力的评价参数为平台的创建能力和平台的资源管理规模，受客观研究实验因素影响，本文虚实互联平台的资源池中包含 255.7 GB 内存、9.1 TB 磁盘、80 个虚拟内核，实际资源管理规模并不算庞大，但本文的虚实互联平台具有良好的可拓展性，可以通过添加部署计算服务的服务器进行平台能力的拓展。

对平台进行批量创建能力测试，实测平台可以在 1 min内进行 40 台虚拟终端节点的创建，如图 8 所示，同时平台支持 1 000 以上的轻量级节点的创建，平台的节点创建能力良好。

4.2　虚实场景构建

通过进行实际场景搭建，测试平台的实用性。

构建测试场景通常需要以测试任务的阶段和需求为依据。一次测试任务往往包含四个阶段：测试计划设计阶段、测试准备阶段、测试执行阶段及测试总结阶段[12]，每个测试阶段包含的测试流程如图 9 所示。为了完成这些测试流程，需要监管员、质量保证员、项目管理员、系统管理员、安全审计员、测试主管及测试员等角色的相互配合[13]。

根据上述需求，可以在虚实互联平台中快速进行测试场景的搭建。首先需要设计测试场景拓扑，根据拓扑生成相应的半结构化的配置文件，并自动创建相应拓扑[14]，如图 10 所示。平台的测试软件可以部署在容器中，供测试人员快速使用。

在该测试环境中网络配置如图 11 所示，其中所有实例都部署于同一子网中，实例之间可以相互连接，同时该子网通过虚拟路由连接至外部网络，可以对外部网络进行访问，并可以通过绑定浮动 IP 实现外部设备的访问，待测设备及软件可以通过该方式连接至测试环境。

通过本文平台搭建的测试环境能够快速轻便地开展测试任务，具有较强的实用性和应用价值[15]。

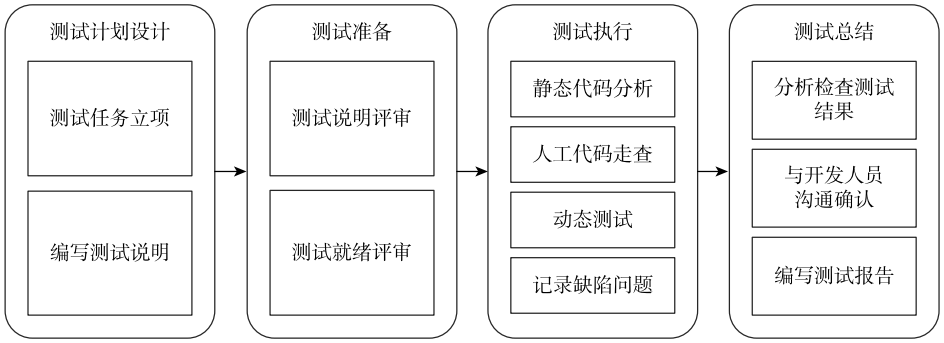


图 9　测试流程

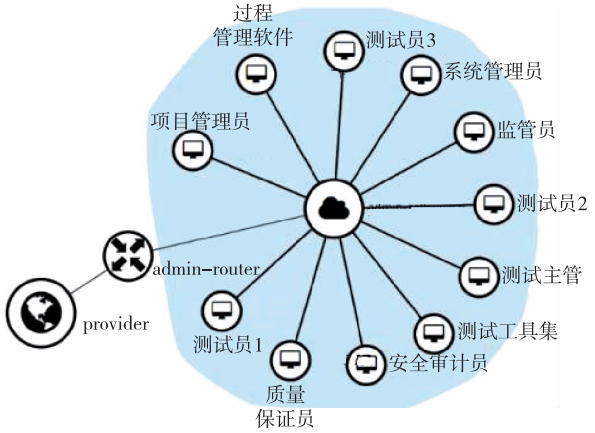


图 10　测试环境拓扑

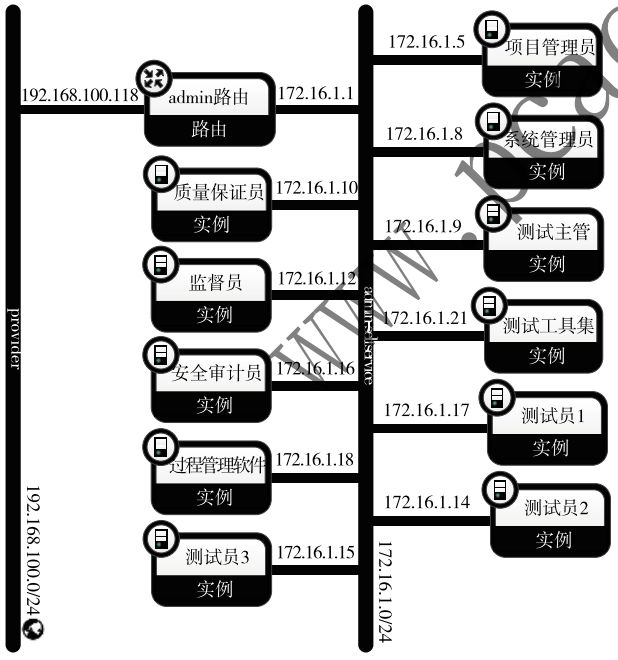


图 11　IP 配置

5　结论

本文通过对现有虚实互联平台研究，针对现有平台的不足，提出一种轻量级安全隔离的虚实互联平台，与现有的三种代表性方法对比具有一定的优势，详细对比如表 1 所示。

表 1　虚实互联平台优势对比

	方法一	方法二	方法三	本文方法
灵活性	√	√	×	√
实用性	√	×	√	√
安全性	×	×	×	√
易拓展	√	√	×	√
轻量级	×	×	×	√

总的来说，通过对虚实互联技术及其应用的研究，能够推进网络仿真技术的发展，从而对复杂场景进行更加逼真的仿真构建。在此基础上，还可以进行更多应用、实践与拓展方面的研究，例如进行其他场景的构建模拟仿真，或在实际应用场景上开展网络对抗训练任务等。对虚实互联技术及其应用的研究具有重要的现实意义与应用价值。

参考文献

[1] 杨继武. 网络虚拟化在云计算领域应用 [J]. 电子技术与软件工程，2019（3）：1.

[2] 肖瑞. 虚实互联场景下网络安全隔离的研究与实现 [D]. 西安：西安电子科技大学，2019.

[3] 冷俊儒. 基于 OpenStack 的大规模虚实互联网络平台设计与实现 [D]. 天津：天津大学，2019.

[4] 李子白，石晶，刘军. 基于 AnyLogic 的跨制式轨道交通网络仿真评价建模应用 [C] //第三十四届中国仿真大会暨第二十一届亚洲仿真会议，2022：575－585.

[5] 李莉，李纪成，张超然，等. 基于 OpenStack 云平台 Neutron 关键技术研究 [J]. 长春理工大学学报（自然科学版），2015，38（6）：114－117.

[6] 陈曦，虞红芳，吴涛，等. 面向教学与科研场景的轻量级网络模拟仿真平台研发及应用实践 [J]. 西南民族大学学报（自然科学版），2023，49（2）：173－179.

[7] 李小宁，李磊，金连文，等. 基于 OpenStack 构建私有云计算平台 [J]. 电信科学，2012，28（9）：1－8.

[8] 陈蕾衣. 基于 OpenStack 的 SDN 控制器优选系统设计与实现 [D]. 成都：西南交通大学，2019.

[9] 邹励豪，董雨鑫，孙建振，等. 基于 OpenStack 平台的 Neutron 服务 [J]. 电脑编程技巧与维护，2020（10）：12－13，46.

[10] MARIA A M，ROSSI T，RASO E，et al. An SDN-based traffic handover control procedure and SGD management logic for EHF satellite networks [J]. Computer Networks，2021，196. DOI：10.1016/j.comnet.2021.108260.

[11] 杨航，郭乔进，吴其华，等. 基于 OpenStack 平台的网络拓扑虚拟静态路由自动配置技术研究 [J]. 信息化研究，2021，47（3）：25－30.

[12] GAROUSI V，FELDERER M，KUHRMANN M，et al. Exploring the industry's challenges in software testing：an empirical study [J]. Journal of Software：Evolution and Process，2020，32（8）. DOI：10.1002/smr.2251.

[13] 张新华，何永前. 软件测试方法概述 [J]. 科技视界，2012（4）：35－37.

[14] BORISENKO O，TURDAKOV D，KUZNETSOV S. Automating cluster creation and management for Apache Spark in OpenStack cloud [J]. Proceedings of the Institute for System Programming of RAS，2018，28（4）. DOI：10.15514/ISPRAS－2014－26（4）－3.

[15] 王超. 云测试是未来趋势——访北京云测信息技术有限公司合伙人及 CMO 张鹏飞 [J]. 信息安全与通信保密，2021（1）：56－59.

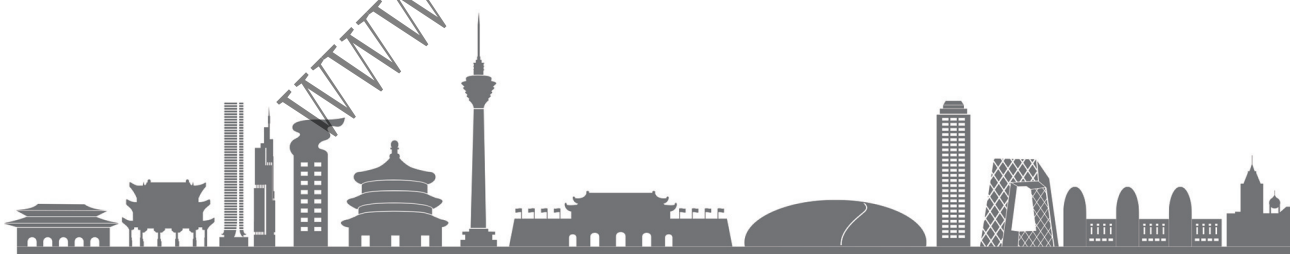
（收稿日期：2023－05－05）

作者简介：

贾星威（1995－），男，硕士，助理工程师，主要研究方向：云安全、深度学习、目标检测。

田晓娜（1988－），女，硕士，工程师，主要研究方向：云安全、工控安全、等保测评。

张宏斌（1989－），男，硕士，高级工程师，主要研究方向：云安全、工控安全。



版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部