DOI 10.15302/J-SSCAE-2020.04.015

面向“互联网 +”的 OT 与 IT 融合发展研究

洪学海 [1,2]，**蔡迪** [1,3]

（1. 中国科学院计算技术研究所，北京 100190；2. 中国科学院计算机网络信息中心，北京 100190；
3. 中国科学院大学计算机科学与技术学院，北京 100049）

摘要：运营技术（OT）与信息技术（IT）的融合成为工业数字化转型和制造业高质量发展的关键。本文开展了 OT 与 IT 融合发展的需求分析，从建立工业物联网、发展跨平台分析框架、开发开放性平台、推行基于云端部署的数据采集与监控系统等方面梳理了 OT 与 IT 融合的现状；提出了建立 OT 与 IT 融合的全套计算栈、持续推进工业互联网、加强 OT 与 IT 融合的安全保障等未来两类技术体系融合的技术路径。研究建议，强化 OT 与 IT 融合的技术标准化应用，建立包括评估关键资产风险、关注底层数据、加强检测系统开发、分离通信功能、应用人工智能技术在内的 OT 与 IT 融合的安全保障体系，以此为我国“互联网 +”行动在工业制造领域的深度发展提供关键支撑。

关键词：互联网 +；运营技术；信息技术；技术融合

中图分类号：TP391　　**文献标识码：**A

Convergence of OT and IT for Internet Plus

Hong Xuehai [1,2] **, Cai Di** [1,3]

(1. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China; 2. Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China; 3. School of Computer Science and Technology, University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: The convergence of operational technology (OT) and information technology (IT) has become the key to industrial digital transformation and high-quality development of the manufacturing industry. This study analyzes the demands for the convergence of OT and IT and summarizes the convergence status of the two technologies from the aspects of industrial Internet of Things, cross-platform analysis framework, open platforms, and supervisory control and data acquisition (SCADA) system based on cloud deployment. It also proposes the technical paths for OT and IT convergence, including establishing a full set of computing stack, continuously promoting the industrial Internet, and strengthening the security assurance. To promote China’s Internet Plus initiative in industrial manufacturing, the standardization of OT and IT convergence should be strengthened, and a security system should be established by conducting risk assessment of key assets, paying attention to underlying data, developing a detecting system with anti-intrusion functions, detaching the communication function, and promoting the application of artificial intelligence.

Keywords: Internet Plus; operational technology; information technology; technology convergence

收稿日期：2020-06-01；**修回日期：**2020-06-29

通讯作者：洪学海，中国科学院计算技术研究所研究员，研究方向为高性能计算、云计算与大数据、信息技术与信息化发展战略；
E-mail: hxh@ict.ac.cn

资助项目：中国工程院咨询项目“‘互联网 +’行动计划战略研究（2035）”(2018-ZD-02)

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

互联网与消费、服务等领域的结合，产生了诸多消费类“互联网 +”应用，促进了我国消费互联网产业的发展。互联网、物联网、大数据、人工智能（AI）、边缘计算、高性能计算等信息技术（IT）越来越多地渗透到工业领域，并与工业技术进行融合发展，产生了以工业互联网为代表的工业“互联网 +”融合应用，这对促进我国工业的数字化转型发展、由制造业大国向制造业强国转变具有重大意义。

OT 即 Operational Technology 的简写，虽然通常翻译为运营技术，究其实质为电子、信息、软件与控制技术的综合运用。OT 可定义为：对企业的各类终端、流程和事件进行监控或控制的软硬件技术，含数据采集和自动控制技术。因此，OT 既包括硬件设施（如机器人、电机、阀门、数控机床等），也包括对这些设施进行控制的各种软件技术。

当前，OT 与 IT 特别是计算技术的融合成为了工业数字化转型与升级的重要方向。IT 与 OT 以及通信技术（CT）正在深度融合，使得工业互联网初步实现了数据和实体的全面联接，推动服务与数据创新，促进数据价值实现，也使实时决策成为可能 [1~5]。本文探讨 IT 与 OT 的融合发展问题，研判 OT 与 IT 技术融合的需求、现状及进展，论证未来 OT 与 IT 技术融合的途径以及 OT 与 IT 融合的安全问题。针对性提出对策建议，以期为我国“互联网 +”行动在工业制造领域的发展研究提供理论参考。

二、OT 与 IT 融合发展的需求分析

朝着数字化转型发展是世界工业大国的主要发力方向，以德国工业 4.0 为代表的一批工业数字化转型战略的发布，标志着工业数字化时代的到来。实现工业数字化转型，关键在于解决 IT 与工业技术的融合问题，而 OT 成为应用瓶颈环节。

OT 与 IT 的融合旨在降低工业成本，优化工业业务流程，降低工业过程风险，更快实施开发和集成，推进通信和控制工业过程设备的标准化。二者融合之后，现有的 IT 软硬件及其环境设备可以便捷地访问 OT 设备及其运行过程数据，OT 设备和过程性数据可以通过 IT 基础设施进行传播，进而在整个企业（或更大的范围）中共享这些设备和过程数据。在运行过程中，可以利用新的 IT 技术（如 AI、边缘计算、区块链等）来快速精准地分析应用工业设备及工业过程数据，进而实现企业信息共享方式的全局优化，为工业制造及其过程管理提供全面的决策支持。

OT 与 IT 的融合能够打通 OT 设备和环境设施数据、IT 基础设施数据，实现双向互用。一方面，OT 系统借助 IT 基础设施获取工业设备及过程的数据，利用 IT 领域的各种算法模型开展 OT 工业设备及过程的状态监控和风险边界预估，有效降低工业组织的潜在风险。另一方面，IT 领域的云和虚拟化等新技术，可以提高 OT 工业设备和过程数据的可访问性、稳定性和流动性。部署通用的 IT 基础设施，兼顾 OT 数据的存储和流动，OT 端可以访问 IT 端的海量数据；在不影响 OT 方面的数据采集与监视控制（SCADA）系统工作的情况下，借助云和虚拟化技术，企业工厂或生产车间的服务器可以迁移到云上，有助于减少设备数量并易于实施更新。

三、OT 与 IT 融合发展的现状

在工业 3.0 时代，OT 和 IT 具有相互独立的界面，二者没有融合的倾向。进入“互联网 +”行动和工业 4.0 时代，OT 与 IT 的融合趋势已经显现，但二者的关系界面决定了融合的程度与方向。关系界面主要表现在功能、领域、访问、资产和人员、变化频率、环境、接口和网络、生命周期、目标、操作系统等 10 个方面，OT 与 IT 融合也主要围绕这 10 个方面展开。目前，工业物联网（IIoT）、工业互联网、基于云的部署等方面是 OT 和 IT 融合的研究重点。

（一）工业物联网

建立 IIoT 是实现 IT 向 OT 融合的关键措施。IIoT 技术蓬勃发展，工业制造企业借鉴物联网技术来部署 IIoT 业务，使得传统工业设备与过程管理朝着物联网方向转型：提出了基于 IIoT 的优化作业车间调度器监控系统，跟踪机器正在执行的任务并闭环反馈路径，据此实现作业完成时间的自动检测以及在此基础上进行的动态重新调度 [6]；发展了

双微控制器（MCU）的架构，确保对可编程控制器（PLC）等 IIoT 设备的弹性控制 [7]；建立了基于单一虚拟化平台、技术高度集成的数据中心网络，具备了支持物联网基础设施的功能 [8]；提出了一种高级分析框架，可作为工矿企业 IIoT 的标准化应用 [9]。

（二）跨平台的分析框架

针对传统工业制造企业的 IIoT 应用需求，市场提供了多种技术和平台的候选方案；但囿于兼容性，企业选择方案通常费时费力。因此，跨平台的分析框架所具有的兼容性优势，可以契合传统制造企业的 IIoT 切实需求。以采矿企业应用为背景，开发了跨平台的分析框架 [10]，集成了 IIoT 和多类先进分析技术，具备将 IIoT 作为分析框架数据来源的功能；通过逐层分析来评定系统性能优劣，易于评估不同架构下的服务和技术，据此实现企业部署方案优选 [9]。

（三）开放性平台

云计算技术的蓬勃发展，促成企业级应用程序和数据从私有平台转移到开放平台。开发开放性平台是应对这一趋势的务实之选。美国通用电气公司（GE）推出的 Predix 基础性系统平台，作为开放性平台可以应用到工业制造、能源、医疗等诸多工业领域，为各类工业设备提供了包括设备健康和故障预测、生产效率优化、能耗管理、排程优化等完备的应用场景；采用数据驱动和机理结合的方式，解决传统工业企业在平衡质量、效率、能耗等方面面临的问题，促进工业企业快速向数字化转型。德国西门子公司（SIEMENS）推出的 MindSphere 平台，采用基于云的开放物联网架构，将传感器、控制器和各种信息系统收集的工业现场设备数据，通过安全通道实时传输到云端，在云端为企业提供大数据分析挖掘、工业应用开发、智能应用增值等服务。文献 [8] 研究了在虚拟化平台上创建技术集成的数据中心网络，支持物联网基础设施运行，为数据中心的物联网应用程序提供了灵活性、可伸缩性和功能拓展能力。

（四）基于云端部署的 SCADA 系统

参照仪器、系统和自动化协会（ISA）制定的企业系统与控制系统集成国际标准 ISA-95，工业自动化模型分为 5 个层次：业务和计划、生产运作管理、监督控制、工厂控制、物理过程。其中，前两个层次归属于 IT 层面，后 3 个层次归属于 OT 层面。监督控制层（即 SCADA 系统所在的层）可视为 IT 与 OT 的分界面，也是 IT 与 OT 实现联接的关键点。如果在这一层面实现了基于云的部署，就可以构建具有用户（或操作员）远程监视（使用传感器）和控制（使用执行器）功能的工业系统，从而大幅提高 OT 与 IT 的联接效率及灵活性。有研究深入分析了 SCADA 系统在云部署时涉及的部署场景 [11]，针对虚拟化、与云数据中心之间附加的网络连接以及因安全措施而增加的计算负载，设计了基准测试系统，获得了不同配置下的云部署 SCADA 系统性能；对云链接的 SCADA 系统建立了模型标准框架，形式化定义了 SCADA 系统的行为 [12]；基于微服务体系结构开发的云化 SCADA 系统，显著提升了 SCADA 系统的性能 [13]。

四、OT 与 IT 融合发展的技术路径预判

OT 与 IT 融合，既能促进 IT 在 OT 端发挥网络化、云化、智能化的作用，也可保障 OT 端更多利用 IT 端的使能技术。融合模式主要分为两类：将 OT 端的信息与 IT 端打通，即建立 IT 端与 OT 端的联接；将 OT 端的信息输出到 IT 端，使得 OT 端信息在更大范围内共享，即 OT 端的信息云化。

OT 与 IT 融合的理想局面，在于追求统一的融合技术框架（如电力行业应用示范 [14]）。为了实现 OT 与 IT 的双向融合，主要从建立全套的计算栈体系、持续发展工业互联网两个路径来推动，同时加强 OT 与 IT 融合的系统安全措施。

（一）建立 IT 与 OT 技术融合的全套计算栈

制造业行业具有产品“量大面广”的特点，制造业生产线装备是 IT 与 OT 技术融合的主战场、工业制造业高质量发展的关键领域。以 PLC、计算机数值控制（CNC）应用为突破口，加强自主可控全套计算栈的研发（见图 1）。在实现 OT 端与 IT 端真正融合、推进 OT 端信息更大范围共享和应用的基础上，以自主可控的全套计算栈来撬动低档生产线装备向中高档的升级（改造）；在努力缩小与国

际先进水平差距的同时，提升我国制造业行业的利润率和国际竞争力，构建适应我国国情的智能装备生态系统。

目前，国外企业和产品依然主导了知识库、设计工具软件、操作系统等诸多方面，但国内产品或开源社区具有替代基础；国外产品主导了处理器芯片市场，但国内有替代技术基础；国内产品主导了其他计算机硬件和应用软件。作为工业设备的计算部件，智能装备计算栈是实现 OT 与 IT 融合的关键之处和必经途径，与工业设备的关系类似于安卓（Android）技术栈与智能手机。

（二）持续推进工业互联网

工业互联网是实现 OT 与 IT 融合的重要载体和关键平台，持续推进相关的技术研发和行业深化应用价值重大。工业互联网的发展历程交织着 IT、OT 与 CT 这 3 条主线 [15]，平台功能架构（见图 2）与云计算架构高度类似，但增加了边缘层；包括基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）在内的关键内容也都类似于云计算。边缘层实质上是生产现场，属于 OT 部分。OT 位于底层，实施数据采集和动作执行；CT 连接所有节点，负责数据传输；IT 位于上层，负责数据运算和分析。

（三）加强 OT 与 IT 融合的安全保障

工业系统从早期的“孤立”状态发展到如今的开放式环境，从最初使用的串行通信发展到当前普遍采用的基于传输控制协议 / 网际协议（TCP/IP）的通信，不可避免地出现了信息安全相关的问题。在 OT 与 IT 融合发展的过程中所面临的安全挑战，主要包括两大方面。

一是 OT 系统自身的缺陷。回顾设计初衷，OT 和关键基础设施是与网络隔离的，因此不会受到来自外部的网络安全威胁。然而历经数字转型之后，这些曾经孤立的系统变成了联网设备，成为攻击者青睐的高价值目标。此外，SCADA、PLC 等面临的安全风险也趋于显现。

二是 OT 与 IT 融合的安全风险。由于 IT 的广泛应用，传统的 OT 设备不再是在孤立网络与专有平台之上独立运行，而是需要与其他系统进行互联互通。二者融合从根本上解决了跨系统的互联互通问题，但带来了诸如外部攻击、内部恶意漏洞攻击、错误操作等潜在的安全风险，具体表现为以下方面。

1. PLCs 安全

PLC 主要面临自主保障和信息安全的问题，且自身设计存在缺陷。PLC 采用扫描式的工作方式（周期为 1~100 ms），在扫描周期结束之前无法进行数据更新（PLC 输入信号时间若小于反应时间，将有误读的可能性）；在每次程序执行之后与下一次程序执行之前输出与输入状态会被更新 1 次（“程序结束再生”），这就给攻击者留下了足够的时间来实施恶意攻击。此外，内存容量小、使用的操作系统存在较大安全隐患、采用的通信协议缺乏安全机制也是导致安全隐患的缺陷因素 [16]。

2. 远程终端单元（RTUs）安全

RTU 是 SCADA 系统的基本单元，面临的安全

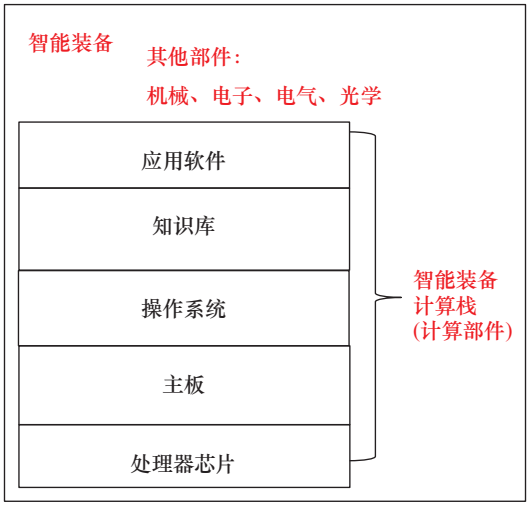

图 1　OT 与 IT 融合的全套计算栈结构示意图

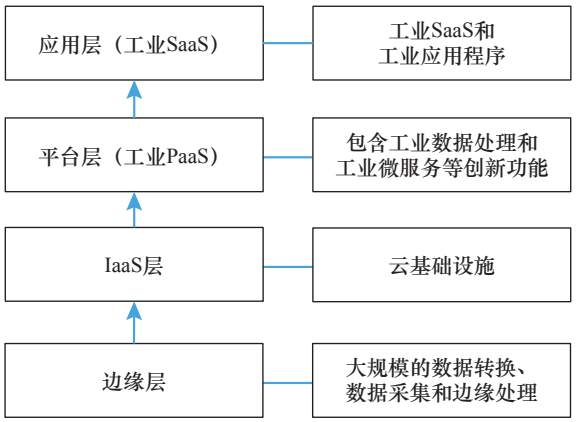

图 2　工业互联网平台功能架构示意图

风险主要来源于：① RTU 软件平台较多采用的嵌入式实时操作系统存在安全漏洞甚至未提供安全监控与防护机制；② SCADA 系统启动后将长期运行、很难及时修复安全漏洞，所在计算机遭遇病毒感染将成为 RTU 设备的安全威胁来源；③ RTU 采用的通信协议缺少安全机制，以明文方式进行信息传输，相应通信过程易被监听和攻击。重点发展网络智能化 RTU 和智能安全 RTU，前者可以提高网络的利用率并实时传输数据，后者要求在数据传输之前加密数据并采用密文形式进行传输。

3. 人机界面（HMI）安全

在工厂规模扩大、组织复杂程度增加的情况下，现场设备的控制精度和准确度成为保障生产的主要因素，这对工业控制的 HMI 产生重大影响。传统 HMI 经历了文本型向图形界面的转变，基本实现了多媒体信息的多样化表达，保障了用户对工业控制现场设备的信息感知和处理能力要求 [17]。然而，HMI、控制 PLC 通常带有密码设置，防止译破密码、偷走程序，保障系统安全，成为 HMI 设计必须面对的关键问题。既要防止产品自身的加密方法存在漏洞，也可将中央处理器与程序存储芯片“二合一”并进行硬件加密，还可取消通信线路的外部接口。

4. SCADA 系统安全

SCADA 系统的安全风险主要来自未授权非法访问、工业控制标准协议和通用技术的开放性、工业控制软硬件产品缺陷、从业人员等方面 [13]。此外，企业由于部署 SCADA 系统的云化，伴生了由云安全延伸而来的系统风险。

五、对策建议

（一）加强 OT 与 IT 融合技术的标准化应用

工业设备种类繁多，接口标准与通信协议标准不够统一，使得针对工业设备及过程的数据采集成为相对复杂的环节。同时，开发统一的融合框架来兼顾各类工业场景需求也较为困难。OT 与 IT 技术融合的标准化建设有待加强。

正在兴起的基于时间敏感网络的 OPC 统一架构（OPC UA over TSN）协议，以其丰富的功能受到各界关注；在解决 OT 与 IT 网络通信标准以及数据格式不统一问题的同时，几乎可以实现“任意的数据访问能力”。因此，结合国内工业企业的实际业务需求，重点开展 OPC UA over TSN 协议的推广使用，对于 OT 与 IT 的融合发展尤为重要。

（二）建立 OT 与 IT 技术融合的安全保障体系

一是实施关键资产风险评估，为系统开发提供关键性的参考。对于重要资产应合理加大保护力度，对于常规资产采取一定力度的防御措施即可。通过合理划分并重点保障，集中防御力量以更加准确、高效地实施系统防护。

二是提高对底层数据的关注度。建议改变当前较多关注源地址、源端口、目的地址、目的端口相关元数据的现象 [18]，转而关注 OT 系统底层和数据传输相关的数据。规避 OT 系统通信安全机制可能存在的漏洞，通过深入理解底层数据来精准保障系统安全。

三是开发具有防入侵能力的检测系统。应重点加强作为系统防护第一道门槛的入侵检测系统研发，检测网络数据包并建立网络入侵行为数据库，保持数据库的及时更新，可以将较大比例的网络攻击拒之门外。

四是分离通信功能。大多数的攻击都是在 OT 与 IT 融合系统进行网络通信时发生的，应将负责网络通信的功能部分从融合系统中分离出来；设计用于网络通信的独立系统，注重与主系统信息交互的安全性。通过这种方式可以很大程度上降低 OT 与 IT 融合系统受到攻击时所面临的风险。

五是加强运用 AI 技术。AI 技术处于新的蓬勃发展阶段，相关技术在 OT 与 IT 融合安全方面可以发挥更大的作用。通过 AI 赋予计算机学习、识别和处理网络攻击行为的能力，发展空间巨大、潜力凸显。

参考文献

[1] 工业和信息化部电子科学技术情报研究所. 工业物联网与工业4.0核心架构 [J]. 新型工业化, 2017, 7(5): 68–69.
Electronic Technology Information Research Institute, MIIT. Industrial Internet of things and Industrial 4.0 core architecture [J]. The Journal of New Industrialization, 2017, 7(5): 68–69

[2] 王振明. SCADA（监控与数据采集）软件系统的设计与开发 [M]. 北京: 机械工业出版社, 2009.
Wang Z M. Design and development of SCADA software system [M]. Beijing: China Machine Press, 2009.

[3] 谭威. 基于PLC的工业控制系统的设计与实现 [D]. 武汉: 华中科技大学(硕士学位论文), 2007.

Tan W. Design and implementation of industrial control system based on PLC [D]. Wuhan: Huazhong University of Science and Technology(Master's thesis), 2007.

[4] 中华人民共和国国家质量监督检验检疫总局, 中国国家标准化管理委员会. 远程终端单元 (RTU) 技术规范 GB/T 34039—2017 [S]. 北京: 中国质量标准出版传媒有限公司, 2018.
General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration. Remote terminal unit (RTU) technical specification GB/T 34039—2017 [S]. Beijing: China Quality and Standards Publishing & Media Co., Ltd., 2018.

[5] 张朝刚. 人机界面交互词的语义研究 [D]. 成都: 西南交通大学(硕士学位论文), 2015.
Zhang C G. Research of the interaction term on human-computer interface [D]. Chengdu: Southwest Jiaotong University(Master's thesis), 2015.

[6] Malik K, Khan S A. IIoT based job shop scheduler monitoring system [C]. Atlanta: The 12th IEEE International Conference on Internet of Things, 2019.

[7] Niedermaier M, Merli D, Sigl G. A secure dual-MCU architecture for robust communication of IIoT devices [C]. Montenegro: 2019 8th Mediterranean Conference on Embedded Computing, 2019.

[8] Petrenko A S, Petrenko S A, Makoveichuk K A, et al. The IIoT/IoT device control model based on narrow-band IoT (NB-IoT) [C]. Moscow and St. Petersburg: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, 2018.

[9] De Moura R L, Ceotto L, Gonzalez A. Industrial IoT and advanced analytics framework: An approach for the mining industry [C]. Las Vegas: The 2017 International Conference on Computational Science and Computational Intelligence, 2017.

[10] Yi M, Mueller H, Yu L, et al. Benchmarking cloud-based SCADA system [C]. Hong Kong: 2017 IEEE 9th International Conference on Cloud Computing Technology and Science, 2017.

[11] Kulik T, Tran-Jorgensen P, Boudjadar J. Compliance verification of a cyber security standard for cloud-connected SCADA [C]. Aarhus: 2019 Global IoT Summit, 2019.

[12] Porrmann T, Essmann R, Colombo A W. Development of an event-oriented, cloud-based SCADA system using a microservice architecture under the RAMI4.0 specification: Lessons learned [C]. Beijing: IECON 2017- 43rd Annual Conference of the IEEE Industrial Electronics Society, 2017.

[13] 黄慧萍. 工业SCADA系统信息安全若干关键技术研究 [D]. 成都: 西南交通大学(博士学位论文), 2016.
Huang H P. Research on some key technologies of information security of industrial SCADA system [D]. Chengdu: Southwest Jiaotong University(Doctoral dissertation), 2016.

[14] Garimella P K. IT-OT integration challenges in utilities [C]. Grugaon: The 2nd International Conference on Communication and Computing Systems, 2018.

[15] 工业互联网产业联盟. 工业互联网体系架构 [R]. 北京: 工业互联网产业联盟, 2016.
Alliance of Industrial Internet. Industrial Internet architecture [R]. Beijing: Alliance of Industrial Internet, 2016.

[16] 徐震, 周晓军, 王利明, 等. PLC攻防关键技术研究进展 [J]. 信息安全学报, 2019, 4(3): 48-69.
Xu Z, Zhou X J, Wang L M, et al. Recent advances in PLC attack and protection technology [J]. Journal of Cyber Security, 2019, 4(3): 48–69.

[17] 王艳愉. 嵌入式人机界面动态构件及存储标准的研究 [D]. 杭州: 杭州电子科技大学(硕士学位论文), 2018.
Wang Y Y. Research on dynamic components and storage standards of embedded human-computer interface [D]. Hangzhou: Hangzhou Dianzi University(Master's thesis), 2018.

[18] Andreu A. Operational technology security—A data perspective [J]. Network Security, 2020 (1): 8–13.