

网络空间公共基础设施体系及安全策略研究

邱洁¹, 韩瑞², 魏志丰², 王志洋¹

(1. 中国互联网络信息中心, 北京 100190;
2. 中国五洲工程设计集团有限公司, 北京 100053)

摘 要: 以物理空间与网络空间的映射关系为研究思路, 面向网络空间的对象、资源、活动等关键要素, 综合考虑了网络空间设备、系统、数据及环境等方面的发展需求, 构建了一种科学的网络空间公共基础设施体系, 并从管理认证和应用认证的双重认证角度出发, 针对用户/设备认证和访问控制等方面给出了一些相应的安全策略和实施建议。

关键词: 网络空间; 公共基础设施; 网络安全; 认证

中图分类号: TP391

文献标识码: A

DOI: 10.11959/j.issn.2096-109x.2021106

Research of public infrastructure system and security policy in cyberspace

QIU Jie¹, HAN Rui², WEI Zhifeng², WANG Zhiyang¹

1. China Internet Network Information Center, Beijing 100190, China
2. China Engineering Group Corporation LTD., 100053, China

Abstract: Considering the key elements, such as object, resources, activities, and other equipment, as same as system, data, environmental and other aspects of demand, the public infrastructure system and security policy between physical space and cyberspace were taken as a basic point. A scientific system of public infrastructure in cyberspace was constructed. From the perspective of dual authentication of management authentication and application authentication, some corresponding safety policies and implementation suggestions were given from the aspects of user/device management and identity authentication.

Keywords: cyberspace, public infrastructure, cybersecurity, certification

收稿日期: 2021-05-26; 修回日期: 2021-07-08

通信作者: 王志洋, wangzhiyang@cnnic.cn

基金项目: 北京市科技新星计划项目 (Z191100001119113)

Foundation Item: The Program of Science and Technology Star in Beijing (Z191100001119113)

论文引用格式: 邱洁, 韩瑞, 魏志丰, 等. 网络空间公共基础设施体系及安全策略研究[J]. 网络与信息安全学报, 2021, 7(6): 56-67.

QIU J, HAN R, WEI Z F, et al. Research of public infrastructure system and security policy in cyberspace[J]. Chinese Journal of Network and Information Security, 2021, 7(6): 56-67.

1 引言

根据2021年2月中国互联网络信息中心发布的第47次《中国互联网络发展状况统计报告》显示,截至2020年12月,我国网民规模已达9.89亿人,约占世界互联网用户总量的20%,互联网普及率达70.4%,超出全球平均水平6.2%^[1]。

网络技术发展方面,基于IPv6的下一代互联网极大提高了网络的容量、效率、速度,推动了许多相关的技术创新,给各行业带来了颠覆性影响^[2-3]。国际发展环境方面,美国于2018年发布了《国家网络战略》,明确将投资5G网络等下一代基础设施^[4]。日本于2019年发布《信息通信白皮书》,重点强调了将基于ICT的改革作为其建设数字经济社会的核心内容,包括移动IP、5G等基础设施建设内容^[5]。欧盟于2019年正式启动了新一轮“数字欧洲计划”,以促进欧洲关键领域的数字基础设施建设和发展^[6],并陆续发布了《欧洲新产业战略》等强调网络信息技术重要性的文件^[7-8]。

面对网络技术和国际环境的快速发展和变化,网络空间面临着诸多挑战。一方面是网络空间连接规模的挑战^[9]。根据2018年Gartner的预测,到2023年,全球物联网连接设备的数量预计将增加至430亿,各类物联网设备将成为网络空间的重要参与对象。另一方面是网络空间治理相关的挑战。随着全球物联网的建设和发展,从物理层、网络层到应用层均需要在传统互联网的基础上进行创新和提升,涉及物联网设备、对象标识及网络协议等领域。如何高效地构建兼容多种用户类型、异构网络协议、多样化管理要求的智慧应用场景,以及如何开展支撑智慧应用场景的各类基础设施管理更成为物联网未来发展亟须解决的关键问题^[10]。

与此同时,网络安全的重要性日益突出。网络安全不仅关系着网络的日常运转,更是国家安全的重要组成部分。各国虽然互联网发展阶段不同、面临的现实挑战不同,但应对网络安全挑战的诉求是一致的,加强网络空间治理的需求也是一致的。

传统的网络安全管理通常是指网络空间中设备、系统、数据、应用等存在的安全问题。面向未来的网络空间安全管理不仅需要包含上述的管

理内容,更需要面对物联网中新出现及未来可能出现的新要素和活动进行开放性的安全规划和设计。以对象要素为切入点,综合考虑网络空间不同资源的本体安全、系统安全、数据安全、行为安全等方面需求,可以更好地支撑网络空间公共基础设施体系的设计。

本文从网络空间载体、资源、主体和操作等网络空间基本组成要素出发,充分借鉴城市公共基础设施体系设计和管理的方法,重点针对网络空间公共基础设施的定义和体系构建进行研究,提出了一种与社会发展相适应的网络空间公共基础设施体系,并结合网络空间公共基础设施的安全发展需求,给出了相应的网络对象管理和身份认证安全策略和方法建议。

2 网络空间公共基础设施及安全相关研究

以城市数字治理为背景,随着网络技术的快速发展和各类对象在网络交往实践中的积极参与,网络空间已经作为一种新的社会空间形态,引起人们的广泛关注。总体来看,网络空间是一种社会空间的体现形式,网络空间的构成是由各种社会力量相互作用而形成的,是现实社会的一种数字表现,其本质是一种社会物理空间的体现形式^[11]。

研究人员针对网络空间及公共基础设施的概念展开了深入的研究工作,目前已形成较为普遍性的认可,但对于网络空间公共基础设施的概念及体系性研究尚不多见。同时,随着物联网的快速发展,传统互联网的信息安全体系同样面临着较大的安全风险挑战,各国围绕物联网环境的发展相关的安全策略均在有序推进,尤其是围绕网络对象和身份管理的研究,网络空间公共基础设施作为重要的网络对象也需要开展相应的研究工作。

2.1 围绕网络空间公共基础设施的概念研究

2.1.1 公共基础设施的概念性研究

为了更好地分析公共基础设施的概念,本文选取较为成熟的城市公共基础设施进行参考性分析。在相关研究领域,被行业研究普遍认可的城市公共基础设施释义是基于世界银行的城市基础设施理论^[12-13]:城市公共基础设施应具有准公共

物品特性。以公共基础设施作为准公共物品的属性特点为基础,学术界从社会空间和组织的维度对公共基础设施进行了定义,通常包含能源、给排水、道路交通、通信、生态环境和抗灾 6 个方面。

在城市公共基础设施的准公共产品定位的基础上,文献[14]提出,公共基础设施是指出于公共目的而建立的,为生产、生活提供公共服务的,能够起到促进社会经济活动、改善生存环境、实现资源共享等作用的各种物质技术条件的总和。

因此,公共基础设施作为所有社会活动和服务的生产所必不可少的要素可按照资源共享、对象的经济活动和生存环境 3 个维度进行分类。

2.1.2 网络空间的概念性研究

文献[15]较为全面地对网络空间概念进行了定义,认为网络空间是创造、存储、调整、交换、共享、提取、使用和消除信息与分散的物质资源的全球动态领域。我国国家重点研发计划“网络空间测绘”中提出,网络空间可被定义为是构建在信息通信技术基础设施之上的一种人造空间,用以支撑人们在该空间中开展各类信息通信技术相关的真实活动^[16]。

针对网络空间的关键资源,国内有学者提出,网络空间是“载体”“信息”“主体”等各类要素的总和,因此网络空间资源不仅包括通信基础设施、应用支撑系统等互联网基础设施实体资源,还包括承载在实体设施之上的内容信息、用户信息等虚拟资源^[17-18]。方滨兴^[19]进一步将网络空间的组成要素分为 4 种类型:载体、信息、主体和操作。综上所述,网络空间的资源和组成要素主要包含载体、信息、主体、操作(创造、存储、调整、交换、共享、提取、使用和消除等)等方面,其对于社会物理空间有促进作用。网络空间的构成如图 1 所示。

在明确了网络空间的基础构成后,进一步结合公共基础设施的特征,可以有助于网络空间公共基础设施的概念分析和定义。本文通过社会物理空间-网络空间的映射关系,从网络空间的基础资源、活动工具和生存环境 3 个方面进行类比分析。

2.2 围绕网络空间安全的关键技术研究

全球物联网的快速发展对网络安全的许多领域提出了挑战。

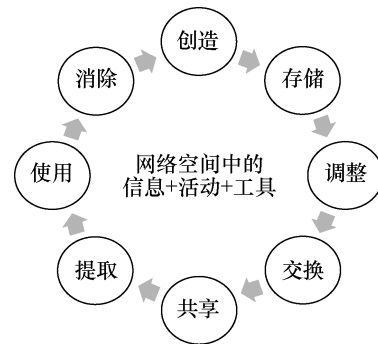


图 1 网络空间的构成

Figure 1 The composition of cyberspace

一方面,物联网设备和应用安全问题尤为突出。物联网中的海量设备需要合理的安全管控机制,其运行和应用活动中会产生大量安全隐私数据,对异构网络的攻击防御问题更加重要。具体到物联网安全接入和控制方面。指出了从互联网到物联网的转变过程中可能会面临的一系列安全问题,并重点强调了普遍存在的资源访问控制问题,针对这些问题相关的安全对策包括:加密机制和密钥管理、感知层鉴别机制、安全路由机制、访问控制机制等^[20]。有研究人员针对物联网感知节点易遭受攻击等物联网安全问题展开了认证和评估方面的研究。目前针对物联网安全认证和访问控制方面的研究包含网络对象的分级管理及基于网络身份的层次化认证等方向^[21]。

另一方面,关键信息基础设施作为国家重要的网络基础设施,其安全受到各国的广泛关注。各国纷纷提出相应的发展战略,将其纳入最高等级的安全保护范围。但在此基础上针对更通用范围的公共基础设施的安全管理机制和规范化研究尚未深入。

2.2.1 网络对象及身份管理相关技术

将分级分类的方法应用到网络用户管理中,对网络身份的可信度及网络身份服务提供商实行等级化管理,已逐渐成为网络对象管理重要的实施方法。邹凯等^[22]提出的智慧城市信息安全风险影响因素体系框架(如图 2 所示)中,将城市信息安全按照环境维度、逻辑维度和组织维度进行了分析。其中组织维度主要是针对网络对象和访问活动进行的分类分析,提出了组织对象的分类等级示例,明确不同的等级应进行不同的权限和活动管理。

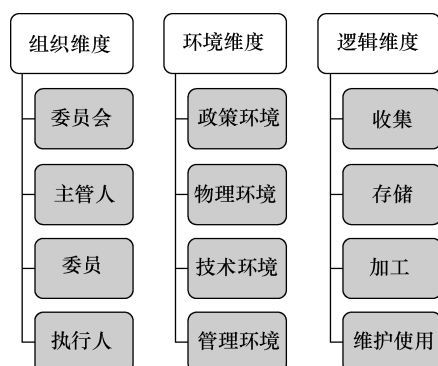


图2 智慧城市信息安全风险影响因素体系框架
Figure 2 The framework of information security influencing factors system in smart city

国际标准化组织 ISO/IEC 等较早开始了关于网络身份管理相关的研究工作，并尝试从风险角度对身份管理的可信等级进行规范，陆续发布了《实体鉴别保障框架》(ISO/IEC 29115-2013)^[23]、《身份核验规范》(ISO/IEC TS 29003:2018)^[24]等标准。该系列标准面向电子商务等活动中的身份管理需求，重点针对身份鉴别过程中与实体身份相关的处理程序、管理活动和技术的可信度进行管理，将身份的可信程度分为3个等级（高、中、低），并规定了4个实体认证保障等别（一级、二级、三级、四级）。ISO/IEC 网络身份管理方案的突出特点是其面向的网络管理对象不限于人、组织等传统网络用户，还包含设备、软件及应用等新的物联网要素。此外，美国、英国等重点针对电子政务管理活动中的身份管理和认证需求相继发布了相关的国家战略^[16]，亚洲各国以电子签名应用技术为基础，围绕电子商务及政府活动中的认证服务陆续开展了相关标准规范的研究工作。相关执行情况如表1所示。

基于网络身份的层次化认证方面，在对无线

传感器网中基于身份的密码体制（IBC，identity-based cryptography）的网络身份认证方案优化的研究中，董发志等^[25]结合无线传感器网的特性，针对IBC中存在的密钥托管、算法安全性等问题，提出了基于身份的分簇认证算法（IDC，identity-based dynamic clustering authentication algorithm），这是一种分层分级处理，一次完成（解）签密的网络身份认证方法，能够降低管理节点的计算量和存储量。危蓉等^[26]提出了采用层簇式密钥管理方式进行无线传感网络会话密钥的管理，该方法采用分层结构将各群体分为不同（区或层）的簇群，如将系统分为簇首层和内部层，由所在基站为每一个簇首统一编发ID号，再由簇首层管理下层节点的身份信息矩阵编号。在分层结构的基础上，有针对性地采用了分级处理，针对簇首、普通节点的功能差异，采用两种不同的公钥生成算法。

在移动物联网场景中，移动IPv6方案也可通过移动锚点来实现对移动节点（MN，mobile node）的分级认证管理。MN认证信息通常存放在家乡网络中，为优化MN的接入认证过程中与家乡网络认证服务器的频繁交互过程，田野等^[27]根据IBC密码方案的实现原理，提出了一种基于身份签名的层次化认证机制，使用HIBS（hierarchical identity-based signature）机制替代传统的基于公钥证书的方式，采用分级的身份标识作为每个节点的公钥。系统由一个根PKG（public key generator）、若干第1层PKG（mobility anchor points 和 home agent）和若干第2层用户（access routers 和 MN等）组成。标识作为每个节点的公钥进行使用，公钥采用多级NAI（network access

表1 网络用户分级管理情况
Table 1 The level management of network users

国家/组织	应用领域	主要内容及要素	管理对象
ISO/IEC	商业领域电子交易活动	身份的可信度、认证过程的可信度划分	人、设备、软件及应用、组织
美国	电子政务	身份的可信度、存在的安全风险划分	人、组织
英国	电子政务	身份的可信度划分	人、活动
欧盟及成员国	商业及公共服务领域	身份的可信度、认证过程的可信度划分	人
韩国、日本	电子商务及政务领域	电子签名的种类及效力划分	人
中国	电子政务、商务及公共服务领域	身份服务过程中存在的风险划分	人、组织

identifier) 标识, 第 1 层是 PKG 身份 ID, 第 2 层是用户身份 ID。通过采用分级的身份, 该方法可以扩展到更多层的认证结构设计中。

此外, 在区块链技术结合网络空间安全研究方面, 张彬等^[28]提出了基于智能合约的无线 Mesh 网络安全架构, 无线网络架构被分为若干区域(如一个园区由多个企业或者一个企业由多个部门共同建立无线网络), 划分区域的目的是便于分级管理, 在每个区域内选择较可靠的路由节点作为管理节点, 它可以是一个管理节点或多个管理节点构成的管理链, 在该管理节点上部署智能合约, 管理所在区域内所有路由节点的公钥, 并实现公钥更新和公钥撤销功能。所有节点共同建立一个联盟合约, 用于记录所有管理节点地址及其上的智能合约地址。该无线网络架构能够较为灵活地实现特定区域内网络服务安全性管理的拓展。

2.2.2 国家关键信息基础设施安全机制

各国面向本国关键信息基础设施的安全管理, 提出了相关的安全管理战略^[29]。美国形成了相对完整的关键信息基础设施安全政策和战略, 并随着形势的变化不断进行优化调整^[30]。欧盟制定了一系列政策, 强调协调成员国加强关键基础设施的网络安全保护方面的重要性^[31-32]。我国国家互联网信息办公室于 2017 发布《关键信息基础设施安全保护条例》, 明确了关键信息基础设施的范围和相关保护要求, 并陆续展开了各类安全保护研究工作^[33], 但针对更大范围的公共基础设施的安全管理机制和规范化研究尚未深入^[34]。此外, 关于网络空间公共基础设施的定义和安全管理方面, 尚未有较成熟和统一的研究成果。

综上所述, 从国家关键信息技术设施到其他网络基础设施, 均已开展系统的安全防护体系研究工作, 本文重点从网络空间公共基础设施的管理视角出发, 研究其系统定义和安全管理。围绕关键的资源、结构和要素, 对网络空间的相关内容和定义进行类比分析, 进而提出网络空间公共基础设施体系的架构和内容。同时, 针对物联网复杂异构环境带来的网络空间的安全问题, 本文将公共基础设施作为网络空间内的典型和关键要素, 重点从设施本身及服务对象的身份管理和认证等方面提出一些相应的策略和建议。

3 网络空间公共基础设施体系设计

3.1 基本构成

结合相关研究情况, 通过社会物理空间-网络空间的映射, 可以从网络空间的基础资源、活动工具和生存环境 3 个方面进行类比分析, 得出网络空间公共基础设施的基本构成, 如图 3 所示。

其中, 网络空间的基础资源主要指网络空间中“载体”“信息”“主体”等各类要素的总和, 因此可以将网络资源进一步细分为标识资源、存储资源、传输资源和计算资源。其中传输资源同时属于网络空间的活动工具。标识资源对应“主体”要素, 相关基础设施包含域名系统、IP 系统、全联网统一标识系统、工业互联网标识系统等公共标识服务系统; 存储资源对应“信息”要素, 相关基础设施包含各级的数据中心、数据库和数据平台等; 计算资源则可以类比为网络空间的基础能力资源, 主要支撑对象的相关活动, 相关基础设施包含公共计算中心、各级计算节点、云计算中心、边缘计算节点、智能终端等。

针对网络空间的活动工具, 主要是支撑信息在网络空间中的“交换”“共享”和“使用”活动所需要的工具, 对应的相关基础设施主要是网络通道和资源接口。其中网络通道为传统的互联网通道, 主要包含无线网络和有线网络通道两方面。资源接口则主要包含数据接口和设备接口两个部分, 数据接口是通过统一平台和相关的应用系统来实现采集接入, 设备接口是通过相对统一的网关或网络交换设备来实现。

针对网络空间的环境要素, 基于物理空间的公共基础设施属性分析方法, 网络空间的环境可以分为生态环境和安全环境两方面, 网络空间的生态环境主要包含网络舆论环境、数据环境、用户环境等方面, 安全环境方面结合能源互联网的安全架构研究^[35], 综合参考 GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》及 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中对网络安全架构及安全保护对象的定义, 主要包含资源层安全和服务层安全两方面。其中, 资源层安全主要对应网络空间资源中的载体、信息和主体, 保护对象为基础

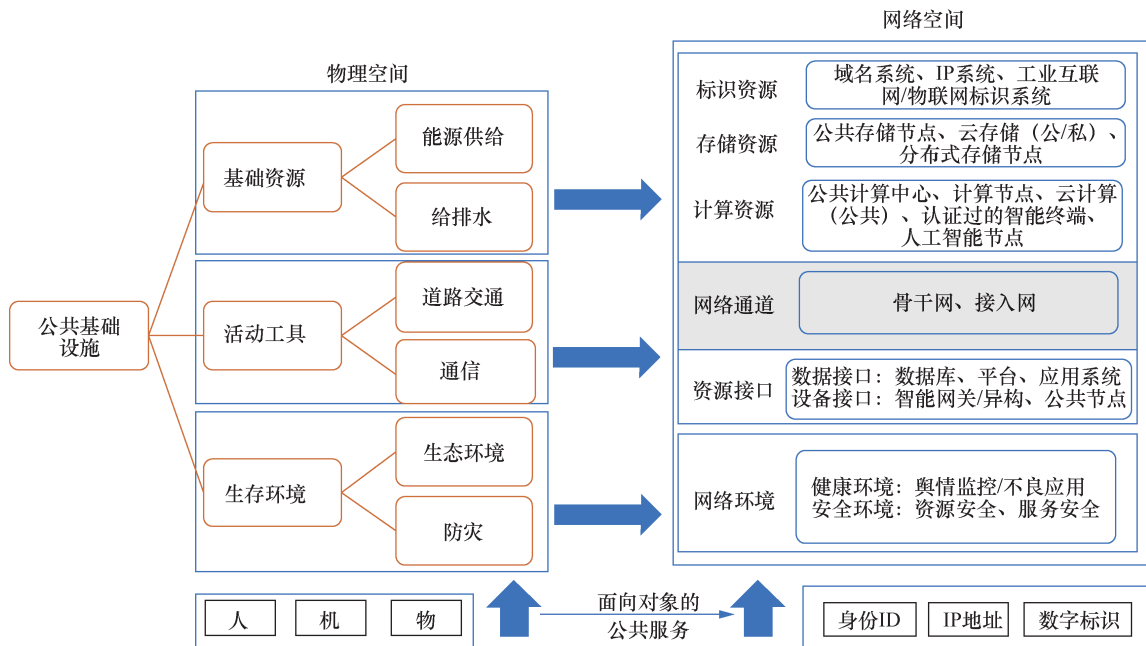


图3 网络空间公共基础设施类比分析

Figure 3 The analogical analysis of public infrastructure in cyberspace

信息网络、物联网、大数据资源、用户身份/标识等；服务层安全主要对应网络空间中的存储、交换、共享、使用等操作活动，保护对象为操作系统、区块链交易系统、云计算平台/系统、大数据平台/系统、工业控制系统、移动应用系统等网络活动的支撑系统。为构建更高效的网络空间运行环境，对于网络空间内安全保护对象的具体保护要求还需要兼顾 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中的等级保护要求（五级）进行设计。

3.2 概念定义

在网络空间公共基础设施的基本构成分析的基础上，根据网络空间的服务内容和属性要求，可以将网络空间公共基础设施定义为：出于公共目的而建立的，为网络空间内生产、生活提供公共服务的，能够起到促进网络空间数字经济活动、改善网络运行环境、实现网络资源共享等作用的各种软硬件设施及技术条件的总和，是维持网络空间高效稳定运行的基础。根据以上定义，可以对网络空间公共基础设施的内容进行识别，明确网络空间公共基础设施的范围边界。

3.3 关键特点

(1) 准公共物品性

大部分网络空间的公共基础设施具有准公共

物品性。一部分人对网络空间内基础设施资源的消费或使用不影响他人的消费或使用。

(2) 服务社会的公共性

为网络空间全范围提供公共的、无处不在的基础服务，供应对象全方位开放，供应能力按需配置。

(3) 经营管理的准集中性

对于关键性的公共基础设施进行高度集中化的管理，对于常规的公共基础设施可以进行分层级分类型的准集中化管理。

(4) 整体架构的系统性

所有网络空间的公共基础设施是一个完整的运行系统，资源、工具和环境要素相互之间通过数据或操作活动相互影响，并不断循环优化和调整形成动态的网络空间。

(5) 配套建设的先行性和基础性

网络空间的公共基础设施是国家网络体系建设的先行和基础工程，应充分考虑与 5G、区块链、人工智能等新一代网络技术、前沿信息技术的兼容性和应用拓展性。

3.4 架构设计

网络空间公共基础设施服务和面向的空间为公共基础空间，是维持网络空间高效稳定运行的基础，因此在建设模式和管理方式上具有一定的集中性。

对注册和认证进行管控，因此在本文的体系架构中其注册管理和认证权限也应为最高级。

面向城市公共行业或网络空间内基础经济运行活动而提供的基础设施纳入公共区管理范围，其通常在特定区域内具有较强的公共服务属性，在管理上通常由地方政府、行业主管部门或授权机构执行，因此注册管理和认证须由相应级别的管理方授权进行，划分为网络空间公共区。

公共基础设施中具有部分公共基础设施属性或为网络空间内部分对象提供其他各类基础服务的基础设施构成了网络空间的开放区环境，该区域内的公共基础设施通常呈现体量大、品类多的特点，因此考虑到实施效率等因素，该区域在建设模式和管理方式上可以更为灵活，注册管理和认证也可以更为自主可控，如可以在分布式

公共基础设施中与国家安全密切相关的基础设施可以纳入国家关键信息基础设施体系进行统筹考虑，在网络空间管理角度该区域为网络空间核心区，如国防、能源、交通、电信等行业的关键信息基础设施。具体内容可以围绕资源、环境和工具进行识别，目前已基本纳入国家关键信息基础设施的管理范畴，在具体执行方面需重点针

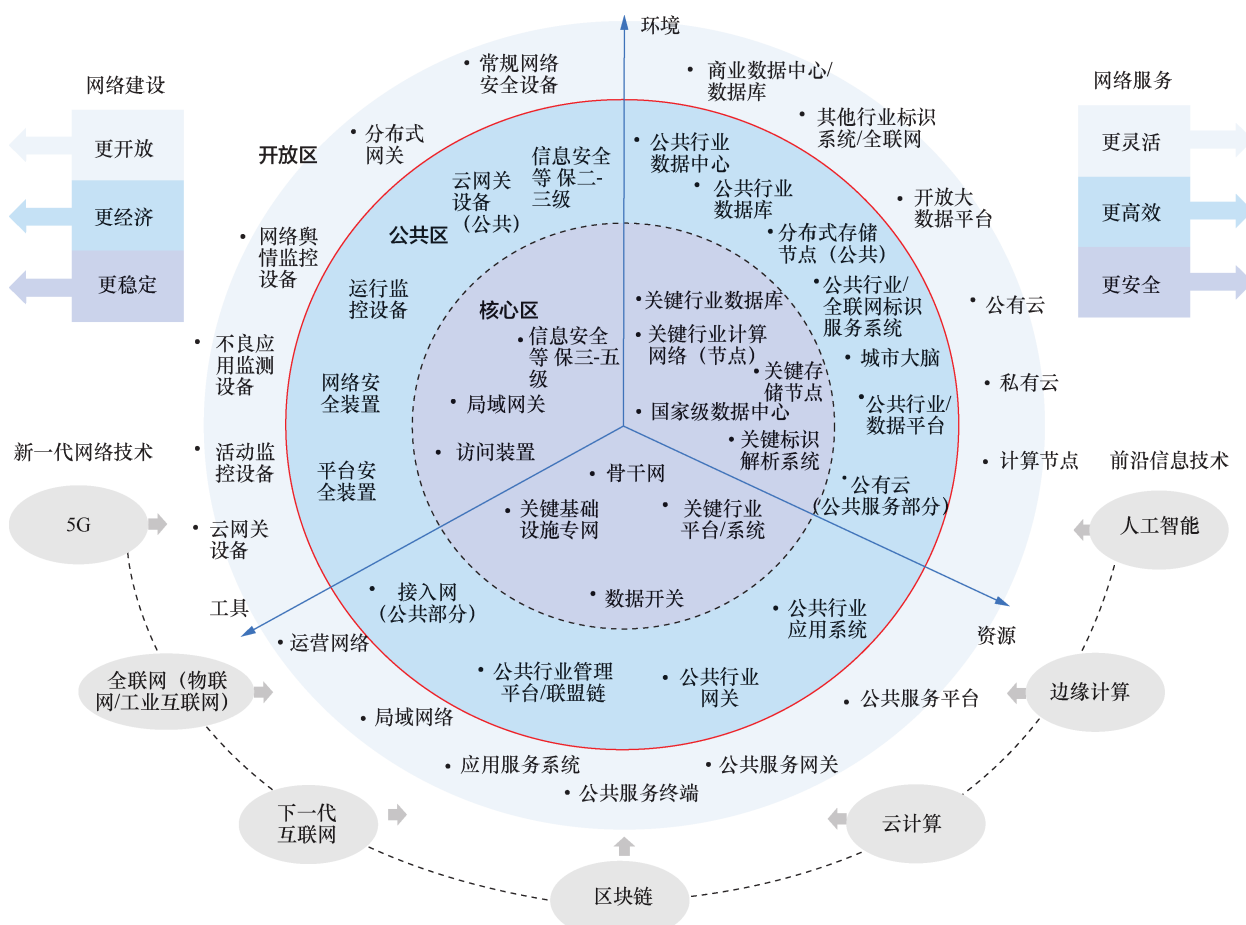


图4 网络空间公共基础设施体系结构

Figure 4 The architecture of public infrastructure system in cyberspace

的终端管理节点进行。

为保障公共基础设施稳定高效运营，底层需要由 5G、全联网（物联网/工业互联网）、下一代互联网等新一代网络技术，及区块链、云计算、边缘计算、人工智能等前沿信息技术提供全面的技术支撑。

3.5 发展目标

基于网络空间公共基础设施的分区规划设计，能够实现我国网络建设和服务方面的提升。

（1）网络建设方面

更开放：通过开放区为服务对象、服务范围及未来技术发展提供更开放的接入环境和发展空间。

更经济：通过对网络空间公共基础设施的统一规划、统筹设计，提高设施在公共服务层面的使用效率，提高设施管理和维护的综合效率。

更稳定：通过分区的公共基础设施空间设计，保障核心区的关键网络空间需求，有利于纳入国家网络空间发展的重要内容。

（2）网络服务方面

更灵活：网络空间公共基础设施可以从对象的环境、工具和资源需求等方面进行效益评估和使用配置，提供更灵活的面向对象服务。

更高效：将网络空间公共基础设施进行集中式+分布式的网络服务构架设计，能够高效利用网络空间内的各类已有基础资源，实现兼容且不断演进。

更安全：将网络空间内具有公共属性的工具和资源进行统一管理，并重点对对象的认证和访问控制进行优化，有助于构建更加安全的网络空间，实现健康的发展和利用。

4 网络空间公共基础设施安全策略研究

在网络空间公共基础设施体系安全环境建设中，既要注重管理政策的规划引导，关注网络空间公共基础设施资源的安全共享机制建设，也要在技术上支撑资源共享活动/设备中的各类用户管理、访问控制等安全保障需求^[38]。

目前针对我国信息化建设的信息系统安全等级保护相关标准规范是实施较为广泛的网络安全规范体系之一。《信息系统安全等级保护基本要求》（GB/T 22239-2008）、《计算机信息系统安全保护等级划分准则》（GB 17859-1999）明确的 5 个等级安全保护设计对不同等级的安全管理要求，主要从访问控制、身份鉴别、标记、数据防篡改、系统可重置、审计、可信路径/恢复等方面进行详细的配置要求，如表 2 所示。其中，访问控制、身份鉴别、标记等方面是重点围绕主体用户控制管理进行的内容设计。

本文充分借鉴网络空间安全相关研究工作基础，以分级的对象管理和认证方法为切入点，提出了与网络空间公共基础设施体系相适应的用户认证和访问控制管理机制建议。

4.1 支持区块链应用的层次化认证管理思路

《计算机信息系统安全保护等级划分准则》将访问控制分为自主访问控制和强制访问控制两个层级。自主访问控制是根据用户指定方式进行授权用户的访问控制。强制访问控制是为用户主体和客体指定统一的敏感标记，该敏感标记是按等级进行的分类，任何访问操作均需要与用户和客体的等级匹配后方可进行访问。

因此，针对现有的访问控制架构进行优化时，可以利用区块链技术安全性、不可逆、不易篡

表 2 计算机信息系统安全保护等级划分准则
Table 2 The criteria for security protection level of computer information system

保护级分类	访问控制		身份鉴别	标记	数据防篡改	系统可重置	可信路径/恢复
	自主访问控制	强制访问控制					
用户自主保护级	√		√		√		
系统审计保护级	√		√		√	√	
安全标记保护级	√	√	√	√	√	√	
结构化保护级	√	√	√	√	√	√	√
访问验证保护级	√	√	√	√	√	√	√

改性和透明性等方面的优势,在不同的访问控制层采用区块链的形式对认证控制(含身份认证和功能认证)服务系统进行组织。例如,顶级访问控制层可以由各行业控制节点按照联盟链结构进行组织,通过智能合约等方式保障信息的准确性,提高身份认证和访问控制的权威性和安全性。

此外,根据实际应用需求还可以在对应层级进行管理节点和普通节点的综合设计,选取某一个或多个服务节点作为管理节点,不同节点按照特定的共识机制和不同的公钥生成/加密方法进行差异化管理。管理节点可以承担用户注册和与上一层级进行认证的交互,以及在本区域内智能合约的管理。其他服务节点为普通节点,仅提供向下的用户注册认证管理服务。

因此,通过去中心化的服务模式可以提高层次化认证架构中身份管理和认证的效率。

4.2 基于区块链架构的管理+功能双重认证机制

以认证管理架构设计为基础,可以将网络空间用户主体和客体的概念拓展到公共基础设施对象上。本文建议公共基础设施以全面的访问控制作为基本要求进行执行,将身份属性验证纳入访问控制消息范围,并进一步将敏感标记的设计根据公共基础设施的管理分配机制纳入应用控制的认证机制中。例如,在接入认证方面,可以对核心区、公共区的公共基础设施按照顶级、行业级和区域级进行设计;在访问控制方面,考虑与区块链及边缘计算技术的结合,通过敏感标记的优化设计综合考虑分级管理的访问权限与城市规划单元中的功能区-街区-地块相结合的组合应用,设置3+3的管理控制和功能控制双重认证机制。

在访问控制管理方面,建议核心区设施由国家指定的业务部门或授权机构执行审核,称为国家网络安全的中心管理节点;公共区由相应的行业主管部门或授权机构执行审核,称为对应的行业管理节点(如电力、电信管理部门等),管理节点可以进一步采用联盟链的形式进行建设。在访问应用服务时则通过识别敏感标记中的权限定义信息,将对应区内设施纳入到区域级的功能节点进行管理,提高管理效率。网络空间访问控制管理架构如图5所示。

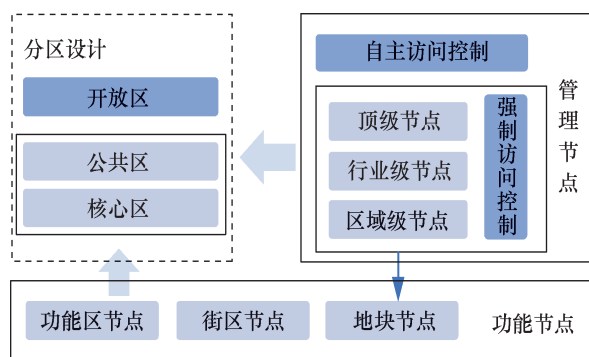


图5 网络空间访问控制管理架构

Figure 5 The architecture of access control management in cyberspace

进一步,可以将网络空间公共基础设施的访问用户按照相应的控制等级及标记要求进行分类对应。例如,核心区关键基础设施的认证对应顶级访问控制节点,其服务对应用户敏感标记中相适应的功能节点。公共区基础设施的管理对应行业控制节点及相应的功能节点,开放区对应区域自主访问控制节点,用户的高、中、低级也可分别与之对应,或者根据实际需求进行更细化的分类。

4.3 双重认证访问控制流程的相关说明

在层次化访问控制设计框架下,对应级别的设施在进行注册和维护管理时,需要向其所对应级别的管理节点进行申请和认证,在进行功能应用时需要向其对应的功能节点进行认证,层次化管理和去中心化服务模式能够较好地满足在服务效率 and 安全性方面的多重要求。

处于公共区的公共基础设施在注册时,需要依次向区域层及行业层提出申请,其交互流程如图6所示。

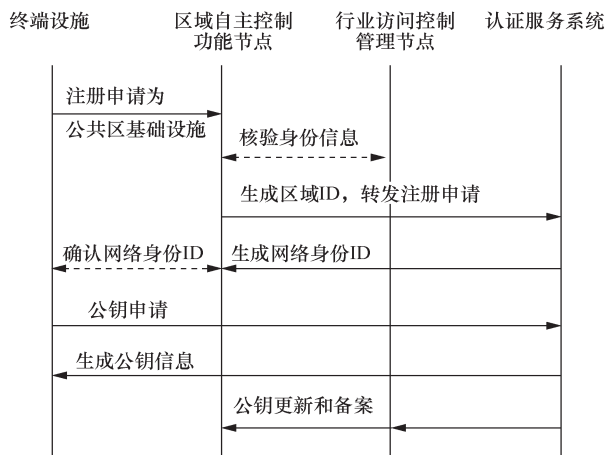


图6 用户交互流程

Figure 6 The process of user interaction

终端设施提出注册申请后，区域控制功能节点向行业访问控制管理节点申请核验身份信息，核验通过后，统一认证服务系统将其生成唯一的网络身份 ID 和敏感标记，并根据节点的类型和等级，采用矩阵运算或哈希函数运算等方法生成基于身份的公钥信息，返回给终端及对应的功能控制节点。

用户申请公共基础设施的网络连接和应用服务前，需获得自身的网络身份 ID，其访问某对象的申请流程为：获得对应级别管理节点的身份认证和敏感标记信息，管理节点将其申请转接对应功能节点的应用认证。例如，某电力公司管理员申请访问城市大数据中心的某项环境监测系统信息，需要通过与城市大数据中心对应行业访问控制节点的认证，并与区域节点进行功能认证后，方可进行网络连接，用户认证流程如图 7 所示。

用户首先通过认证服务系统客户端验证和查询对应的区域节点地址，根据反馈情况向区域功能节点发起认证申请，可以陆续基于其公钥信息在区域自主控制功能节点及行业控制管理节点进行客户端合约认证和认证服务系统侧访问认证等安全控制操作，并通过其敏感标记信息完成与访问对象的区域功能节点的功能认证后，实现目标设备的访问。

在上述管理模式的基础上，公共基础设施及用户还可以通过统一的网络空间身份编码进行标识，将敏感标记中其对应的用户身份级别和类型

信息纳入其中，也可以将该标识作为公钥在身份认证过程中进行使用，以提高密钥管理和身份认证过程的效率。

5 结束语

本文充分借鉴了城市公共基础设施体系的相关理论和设计方法，分析了公共基础设施作为准公共物品属性，在网络空间内的基础资源、活动工具、运行环境等方面应该覆盖的内容和边界；明确了网络空间公共基础设施的内涵，并基于此提出了网络空间公共基础设施体系分区化管理的概念，在总体架构中按照核心区、公共区和开放区进行分区分层的设计。此外，本文从网络空间安全管理角度出发，重点针对网络空间安全中的组织安全管理需求，在网络空间公共基础设施层次化管理架构和认证流程设计等方面提出了一些具体的组织方法和建议，具有较强的可实施性和应用拓展性。

参考文献：

- [1] CNNIC. Statistical report on internet development in China[R]. 2021.
- [2] ANBAR M, ABDULLAH R, AL-TAMIMI B N, et al. A machine learning approach to detect router advertisement flooding attacks in next-generation IPv6 networks[J]. Cognitive Computation, 2018, 10(2): 201-214.
- [3] China Mobile Internet Development Report (2020)[R]. 2020.

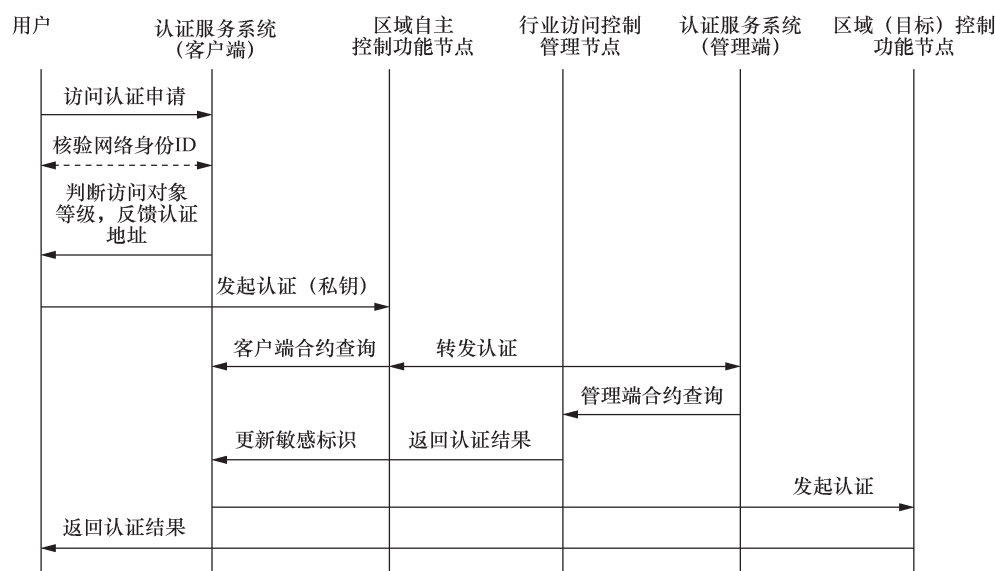


图 7 用户认证流程

Figure 7 The process of user authentication

- [4] TERRI MOON CRONK. White house releases first national cyber strategy in 15 years[R]. 2018.
- [5] Economic Research Office. Overview of the 2019 White Paper on Information and Communications in Japan[R]. 2019.
- [6] THOMAS B. Towards a common 5G strategy: the case for UK-Germany collaboration[R]. 2020.
- [7] POTOČNIK J. Recover today, lead for 2030: a future-fit industrial strategy for Europe[R]. 2021.
- [8] The Ministry of Finance. Government Standard No.5-Public Infrastructure[S]. 2017.
- [9] GEORGE K. IoT analytics[EB]. 2018.
- [10] GU Y, REN F J, JI Y S, et al. The evolution of sink mobility management in wireless sensor networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2016, 18(1): 507-524.
- [11] 陈宗章. 网络空间: 概念、特征及其空间归属[J]. 重庆邮电大学学报(社会科学版), 2019, 31(2): 63-71.
CHEN Z Z. Cyberspace: conception, characteristics and its attribution[J]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 2019, 31(2): 63-71.
- [12] 韩传峰. 城市公共服务设施的一类价值评估计算模型[J]. 同济大学学报(自然科学版), 2004, 32(9): 1239-1251.
HAN C F. Computing model in evaluation on city public service Establishment[J]. Journal of Tongji University (Natural Science). 2004, 32(9): 1239-1251.
- [13] 徐翀崎, 李锋, 韩宝龙. 城市生态基础设施管理研究进展[J]. 生态学报, 2016, 36(11): 3146-3155.
XU C Q, LI F, HAN B L. Progress in research on urban ecological infrastructure management[J]. Acta Ecologica Sinica, 2016, 36(11): 3146-3155.
- [14] 王坤岩. 城市公共基础设施效益三维度评价研究[M]. 北京: 企业管理出版社, 2017.
WANG K Y. Study on three-dimensional evaluation of urban public infrastructure benefit[M]. Beijing: Enterprise Management Publishing House.
- [15] KITCHIN R M. Towards geographies of cyberspace[J]. Progress in Human Geography, 1998, 22(3): 385-406.
- [16] 郭莉, 曹亚男, 苏马婧, 等. 网络空间资源测绘: 概念与技术[J]. 信息安全学报, 2018, 3(4): 1-14.
GUO L, CAO Y N, SU M J, et al. Cyberspace resources surveying and mapping: the concepts and technologies[J]. Journal of Cyber Security, 2018, 3(4): 1-14.
- [17] 张江, 孙治, 徐锐, 等. 一种网络空间资源的测度方法研究[J]. 信息技术与网络安全, 2019, 38(5): 7-11.
ZHANG J, SUN Z, XU R, et al. A research on measure method of cyberspace resource[J]. Information Technology and Network Security, 2019, 38(5): 7-11.
- [18] CHEN Z Z. Cyberspace: conception, characteristics and its attribution[J]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 2019, 31(2): 63-71.
- [19] 方滨兴. 定义网络空间安全[J]. 网络与信息安全学报, 2018, 4(1): 1-5.
- FANG B X. Define cyberspace security[J]. Chinese Journal of Network and Information Security, 2018, 4(1): 1-5.
- [20] OLIVEIRA L B, DAHAB R, LOPEZ J, et al. Identity-based encryption for sensor networks[C]//Proceedings of Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07). 2007: 290-294.
- [21] ROHBANIAN M R, KHARAZMI M R, KESHAVARZ-HADDAD A, et al. Watchdog- LEACH: a new method based on LEACH protocol to secure clustered wireless sensor networks[J]. Advances in Computer Science An International Journal, 2013, 2(3): 105-117.
- [22] 邹凯, 侯岚, 蒋知义, 等. 智慧城市信息安全风险影响因素的三维结构框架与识别研究[J]. 现代情报, 2019, 39(10): 15-23.
ZOU K, HOU L, JIANG Z Y, et al. Research on 3-D structure and recognition of influencing factors of information security risk in smart city[J]. Journal of Modern Information, 2019, 39(10): 15-23.
- [23] ISO/IEC 29115-2013. Information technology-security techniques-entity authentication assurance framework[S]. 2013
- [24] ISO/IEC TS 29003:2018. Information technology-security techniques -Identity proofing[S]. 2018
- [25] 董发志, 丁洪伟, 杨志军, 等. 基于遗传算法和模糊 C 均值聚类 WSN 分簇路由算法[J]. 计算机应用, 2019, 39(8): 2359-2365.
DONG F Z, DING H W, YANG Z J, et al. WSN clustering routing algorithm based on genetic algorithm and fuzzy C-means clustering[J]. Journal of Computer Applications, 2019, 39(8): 2359-2365.
- [26] 危蓉, 赵德正. 基于身份的无线传感器网络层簇式密钥管理方案[J]. 武汉大学学报(工学版), 2015, 48(4): 580-583, 590.
WEI R, ZHAO D Z. Key-management scheme based on identity and cluster layer for wireless sensor network[J]. Engineering Journal of Wuhan University, 2015, 48(4): 580-583, 590.
- [27] 田野, 张玉军, 张瀚文, 等. 移动 IPv6 网络基于身份的层次化接入认证机制[J]. 计算机学报, 2007, 30(6): 905-915.
TIAN Y, ZHANG Y J, ZHANG H W, et al. Identity-based hierarchical access authentication in mobile IPv6 network[J]. Chinese Journal of Computers, 2007, 30(6): 905-915.
- [28] 张彬, 广晖, 陈熹. 基于智能合约的无线 Mesh 网络安全架构[J]. 计算机工程, 2019, 45(11): 16-23, 31.
ZHANG B, GUANG H, CHEN X. Smart contract-based security architecture for wireless mesh network[J]. Computer Engineering, 2019, 45(11): 16-23, 31.
- [29] CAO J W, YANG M B. Energy Internet: towards smart grid 2.0[C]//Proceedings of 2013 Fourth International Conference on Networking and Distributed Computing. Piscataway: IEEE Press, 2013: 105-110
- [30] XU G Q, CAO Y, REN Y Y, et al. Network security situation awareness based on semantic ontology and user-defined rules for Internet of Things[J]. IEEE Access, 2017, 5: 21046-21056.
- [31] HÄNISCH T, ROGGE S. IT-Sicherheit in der Industrie 4.0[M]. Wiesbaden, Germany: Springer, 2017.
- [32] European Commission. EU cyber security strategy [R]. 2018.
- [33] 董亚南, 赵改侠, 谢宗晓. 关键信息基础设施保护及其实践探讨[J].

网络空间安全, 2018, 9(8): 84-89.

DONG Y N, ZHAO G X, XIE Z X. The practice of critical information infrastructure protection analysis[J]. Cyberspace Security, 2018, 9(8): 84-89.

- [34] 郭朝先, 刘艳红. 中国信息基础设施建设: 成就、差距与对策[J]. 企业经济, 2020, 39(9): 143-151.

GUO C X, LIU Y H. The construction, achievements, gaps and countermeasures of information infrastructure in China[J]. Enterprise Economy, 2020, 39(9): 143-151.

- [35] SANI A S, YUAN D, JIN J, et al. Cyber security framework for Internet of Things-based Energy Internet[J]. Future Generation Computer Systems, 2019, 93: 849-859.

- [36] TECHNOLOGY N I O S A. Framework for improving critical infrastructure cybersecurity: version 1.0[EB]. 2014.

- [37] STINE K, BARRETT M. Portuguese translation of the framework for improving critical infrastructure cybersecurity version 1.1 (cybersecurity framework)[R]. National Institute of Standards and Technology, 2021.

- [38] European Network and Information Security Agency. EU network and information security directive[R]. 2019.

[作者简介]



邱洁(1986-), 女, 江西吉安人, 中国互联网络信息中心高级工程师, 主要研究方向为智慧城市、物联网标识应用及安全、信息基础设施管理。

韩瑞(1979-), 男, 河北唐山人, 中国五洲工程设计集团有限公司高级工程师, 主要研究方向为工业互联网安全。

魏志丰(1971-), 男, 黑龙江大庆人, 中国五洲工程设计集团有限公司高级工程师, 主要研究方向为工业互联网安全。

王志洋(1984-), 男, 安徽枞阳人, 博士, 中国互联网络信息中心高级工程师, 主要研究方向为大数据分析、标识解析技术、互联网基础资源管理。