物联网安全标准体系框架研究

李　峰，陈　亮，李　凯，王亚玲
（军事科学院系统工程研究院 后勤科学与技术研究所，北京 100166）

摘　要： 结合物联网发展标准化需要，概述了国际国内物联网安全标准化组织，从技术和应用视角对物联网安全标准进行了分类，设计了物联网安全标准体系框架，并针对性提出了物联网安全标准化推进建议。

关键词： 物联网安全；标准体系框架
中图分类号： TP39；T-65　　**文献标识码：** A　　DOI：10.16157/j.issn.0258-7998.212270

中文引用格式： 李峰，陈亮，李凯，等. 物联网安全标准体系框架研究[J].电子技术应用，2022，48(7)：8-12.
英文引用格式： Li Feng，Chen Liang，Li Kai，et al. Research on the framework of the security standard system of the Internet of Things[J]. Application of Electronic Technique，2022，48(7)：8-12.

Research on the framework of the security standard system of the Internet of Things

Li Feng，Chen Liang，Li Kai，Wang Yaling
(Logistics Science and Technology Institute，Institute of System Engineering，Academy of Military Sciences of the CPLA，Beijing 100166，China)

Abstract： In combination with the standardization needs of the development of the Internet of Things，this paper outlines the international and domestic Internet of Things security standardization organizations. From the perspective of technology and application，the Internet of Things security standards are classified. Finally，this paper designs the framework of the Internet of Things security standard system，and puts forward recommendations for the advancement of security standardization of the Internet of Things.

Key words： Internet of Things security；standard system framework

0 引言

物联网历经几十年的发展，其概念、特征与作用逐步取得全球的共识。2015 年国际电信联盟(ITU)把物联网定义为“信息社会全球基础设施(通过物理和虚拟手段)将基于现有和正在出现的、信息互操作和通信技术的物质相互连接，以提供先进的服务”[1]。近年来随着技术成熟度越来越高，物联网已被广泛应用于农业、能源、交通、医疗、家居、军事等领域，推动了经济与社会发展，2021 年度《中国互联网发展报告》指出，物联网市场规模已经达到 1.7 万亿元[2]。然而，由于物联网终端设备具有空间分布广、应用环境复杂、设备资源薄弱等特点，带来了安全防护措施不全、安全防护能力薄弱、隐私保护不充分等问题，通常认为物联网比传统网络面临更加严重的安全威胁[3]。物联网安全标准是保护物联网系统减轻安全威胁，实现设备联网入网，进行数据采集、传输与利用的基础支撑，是物联网标准体系的重要组成。

本文在阐述物联网安全标准内外关系的同时，概述了国际国内物联网安全标准化主要组织，并对物联网安全标准进行了分类；给出了物联网安全标准体系框架；提出了物联网安全标准化推进建议；最后对全文进行了总结。

1 物联网安全标准及其分类

1.1 物联网安全标准化组织

为加强物联网技术安全研究和应用，国际国内均成立了相关标准化组织，国际上有影响力的包括 ISO/IEC JTC1/SC27(信息技术委员会/安全技术分委员会)、SC41(物联网及相关技术分委员会)、SC25(信息技术设备互联分委员会)，ITU-T SG17(安全研究组)、SG20/Q6(物联网和智慧城市研究组/安全、隐私保护、信任和识别课题组)，ETSI(欧洲电信标准化协会)，国内则主要有全国信息安全标准化技术委员会(SAC/TC260)、中国通信标准化协会(CCSA)、车载信息服务产业应用联盟(TIAA)、工业互联网产业联盟(AII)等[4]。

其中，ISO/IEC 下辖相关物联网安全分委员会，主要侧重物联网信息安全、智能家居、隐私保护等类别技术安全标准研究与制定，ITU-T 则更为关注物联网通信安全、智慧城市、信任和识别等相关物联网安全类标准制修订，ETSI 更多倾向于消费类物联网安全标准应用。我国则以全国信息安全标准化技术委员会为物联网安全标准主要归口，其于 2018 年 12 月 28 日发布的 27 项国家标准[5]，涉及物联网安全方面的有 5 项，分别为：

GB/T 37044－2018《信息安全技术 物联网安全参考模型及通用要求》、GB/T 36951－2018《信息安全技术 物联网感知终端应用安全技术要求》、GB/T 37024－2018《信息安全技术 物联网感知层网关安全技术要求》、GB/T 37025－2018《信息安全技术 物联网数据传输安全技术要求》、GB/T 37093－2018《信息安全技术 物联网感知层接入通信网的安全要求》，主要是参考了国际上物联网3层架构和国内物联网“六域模型”架构[6-7]，明确了物联网的安全对象和安全责任，提出了感知层、物联网网关、接入通信网和数据传输等方面的标准化要求，总结了应用层和网络层使用等级保护相关标准。

1.2 物联网安全标准的分类

从不同的维度可以把物联网安全标准划分到不同的分类体系中，结合物联网属性特征，本文从技术和应用两个维度对物联网安全标准进行分类。

1.2.1 技术视角物联网安全标准分类

参考国际通用的物联网感知、传输与应用三层体系架构，综合考虑安全标准体系涉及的基础术语与模型和物联网技术应用实际，从技术视角可把物联网标准划分为4类，分别是基础通用类、传感采集类、通信传输类、应用管理类，如图1所示。

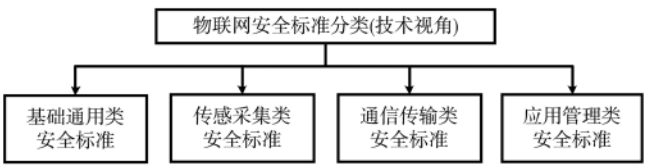

图1 物联网安全标准分类(技术视角)

其中，基础通用类包括术语、概念、模型、框架等物联网安全技术与应用需要统一描述和定义的基础性内容；传感采集类包括传感器安全、芯片卡安全、物联网终端安全以及集成网关安全等内容；通信传输类包括有线无线通信安全、网络数据安全交换、数据传输与隐私防护防篡改等内容；应用管理类包括应用安全规范、数据安全使用、运维管理安全以及与新技术整合安全等内容。

1.2.2 应用视角物联网安全标准分类

结合物联网支撑工业互联网、智慧城市、智慧物流、车联网等行业社会经济实践活动，从应用视角可把物联网安全标准分为基础综合类、应用要求类、实施指南类与检测评估类4种类型，如图2所示。

其中，基础综合类包括基础性的符号、术语，以及综合性的安全防护框架等；应用要求类通常结合行业物联网应用特点，针对不同领域提出不同的物联网技术应用实施安全防护要求，例如，医疗设备类物联网安全标准与农业物联网安全标准相关安全防护要求差异较大[8-9]，需要分别提出相应的物联网安全应用标准；实施指南类包括不同行业领域不同应用类型物联网安全应用实施需要遵循的网络拓扑、信息流程或操作注意事项等强制或参考性安全内容；检测评估类包括安全测试与检测，以及针对场景类别，结合不同的安全防护等级制定的安全评估类标准。

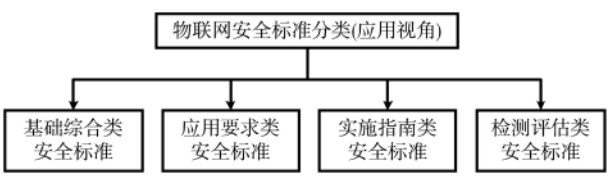

图2 物联网安全标准分类(应用视角)

1.2.3 物联网安全标准的外延

物联网最早是在传统的电信和互联网领域发展起来的，随着概念内涵的不断深化，其与当前的5G/6G、云计算与大数据、人工智能、区块链等新兴技术的应用发展紧密关联；从应用层面物联网与众多新兴技术综合集成共同支撑工业互联网、智慧城市、智慧物流、车联网等行业发展。因此，物联网安全标准与这些关联技术体系和应用密切相关。即，物联网安全标准体系框架构建，需要参考相关技术领域安全标准，包括传统通信与网络安全标准和新技术相关安全标准，能直接采用的应直接采用，需要制修订的应尽可能保持兼容，同时在行业应用领域方面与安全要求相配套，并能够支撑各行业新兴应用。对应的外延关系如图3所示[10]。

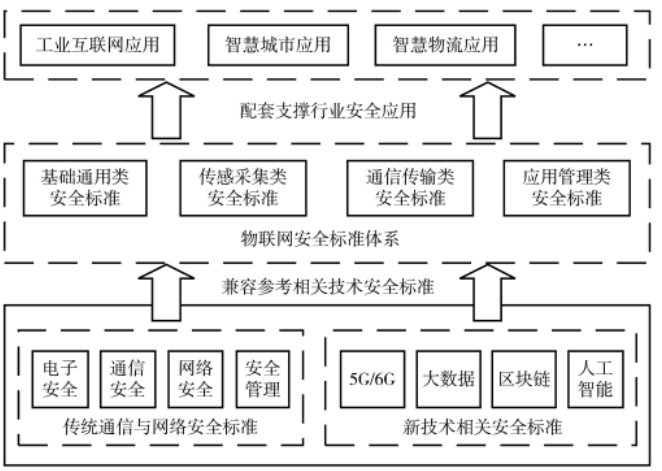

图3 物联网安全标准的外延

2 物联网安全标准体系框架

2.1 物联网安全标准总体框架

结合物联网安全标准的分类，本文依据前文1.2.1小结提出的技术视角物联网安全标准分类，进一步细化形成物联网安全标准体系框架，如图4所示。

基础通用类主要包括物联网安全概念与术语、物联网安全参考模型、物联网安全框架三个小类的安全标准，传感采集类主要包括传感器安全、控制器安全、智能卡及芯片安全、智能终端安全、网关与边缘计算安全等子类别的安全标准，通信传输类包括有线通信、无线通信、数据交换、数据传输与隐私防护4个小类的安全标准，

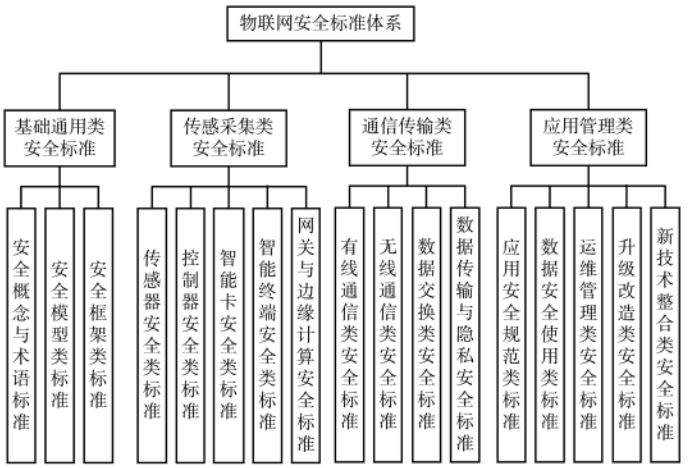

图 4 物联网安全标准体系框架

应用管理类包括应用安全规范、数据安全使用、物联网运维管理、物联网升级改造、新技术整合应用共 5 个小类的安全标准。

2.2 基础通用类安全标准

基础通用类安全标准主要用于解决物联网安全领域概念术语统一性、参考模型兼容性和安全框架一致性的问题，用于避免出现安全标准制修订混乱、技术安全不兼容和应用安全框架认知不一致等现象[11]。

物联网安全概念与术语类标准主要是为物联网安全领域交流、使用提供一致性的语言载体，达成共同的语言认知，该类标准的制定应注意术语专业性和通用性的平衡，既能够为专业人员交流提供准确表达的手段，又能够为更多的行业初学者提供简单易记的术语。例如，AMQP(高级消息队列协议)术语，是指一个开源标准，用于不同的应用程序在任何网络和任何设备之间进行通信[12]；MQTT(MQ 遥测传输)术语，是指一种发布/订阅消息协议，用于在设备相互通信的情况下使用有限的计算能力，或者在不可靠或延迟的网络连接的情况下使用[13]。物联网安全参考模型类标准，用于提供标准化的物联网安全模型，供物联网安全实践过程中参考和应用。例如，GB/T 37044-2018《信息安全技术 物联网安全参考模型及通用要求》提出了由参考安全分区、基本安全防护措施和系统生成周期三个维度共同组成的物联网安全参考模型，同时每个维度包含了不同的阶段，为物联网其他安全标准制定以及物联网安全防护实践提供了重要参考[14]。物联网安全框架类标准，用于明确物联网安全功能组成要素，以及各功能要素之间的逻辑组成、层次结构、拓扑架构和影响关系，通常作为物联网感知采集、通信传输和应用管理类安全标准制定的框架参考，便于物联网安全从业者快速了解并遵循相关的物联网安全框架要求。

2.3 传感采集类安全标准

传感采集类安全标准主要是为物联网感知层各类传感器、控制器、网关、智能终端以及边缘计算设备与相关嵌入式系统或软件提供相对应的技术设计、应用防护和安全操作等相关标准。

传感器安全类标准主要用于满足或指导各类日常或严苛条件下传感器物理部署安全、感知节点信任鉴权安全、传感量程干扰安全、电磁攻击安全、传感信息伪造或篡改安全等，也可按照传感数据量、传感数据报送频度进行相关安全标准制定；控制器安全类标准通常包括控制器防伪、短距离信息安全鉴权、防止信息伪造和重放攻击等安全标准内容，例如智能门锁、电子门禁安全标准等；智能卡及芯片安全类标准，随着芯片存储容量和性能的提升带来的物联网大规模应用，这类安全标准种类较为丰富，通常包括卡片物理芯片安全，芯片访问鉴权、存储分区、数据保护、加密模块及密钥，假冒、嗅探、重放、拒绝服务等系列安全标准内容；智能终端是近几年迅速发展起来的具备一定计算与存储能力的物联网产品[14]，其相关安全类标准与嵌入式设备、智能电子设备之间存在较多的交叉，包括环境类、通信类、数据类、应用类和身份鉴别类等安全标准；网关与边缘计算节点通常部署在物联网感知层与传输层的交界[15]，是数据汇总上传和关键反馈控制指令下达的枢纽，其安全类标准主要用于满足设备鉴权接入、信息存储、数据共享交换、协议转换、数据过滤压缩、嵌入式计算环境等安全防护需要。

2.4 通信传输类安全标准

通信传输类安全标准是基于有线网络和无线网络通信提供技术与应用安全的相关标准，例如针对烟花爆竹类库房物联网、无人机自组网、机器人体域网等应用场景下安全通信制定的传输、交换、隐私保护等相关标准。

有线通信类安全标准，包括传统的有线通信安全标准，例如 RS232 串口、RS-485 串行总线，以及物联网固定网络接入等安全标准，也包括新增的物联网相关的有限通信类安全标准，例如 USB 3.0 安全标准[16]等；无线通信类安全标准，是指蓝牙、ZigBee、Lora、NB-IoT、Wi-Fi、IPv6/6Lowpan 等物联网无线通信类安全标准，这些标准通常需要包括接入鉴权、空口协议、通信协议、数据保护、密钥管理、安全审计等相关内容，同时由于技术的交叉性，这些安全标准通常按通信类型来分类。

物联网数据的传输通常要跨越不同的网络类型，同时在数据流向上既有单向跨网也有双向流动，与单一网络相比面临更加严重的信息安全威胁。数据交换安全标准，旨在为数据交换起点、过程和终点提供访问鉴权、数据加解密、一致性和完整性校验、数据自毁、密钥管理等系列安全防护内容，为物联网数据交换提供安全保障；数据传输与隐私安全标准，通常包括传输协议安全、传输算法破解、中间人攻击以及用户隐私访问控制等内容，例如，可穿戴医疗设备安全标准应考虑中间人复制用户敏感隐私信息。

2.5 应用管理类安全标准

应用管理类安全标准是为物联网技术与产品的操作使用、物联网数据的业务应用、物联网全生命周期的运维管理、物联网的升级改造以及物联网与新技术的整合应用提供系列安全类标准。

应用安全规范类安全标准，是面向物联网产品设计和研发人员以及操作维护人员等制定的，包括并不仅限于为物联网数据、技术以及产品应用而制定的系列安全标准或规范，指导物联网从业人员在安全许可范围内进行各类物联网建设和管理，目的在于通过统一的标准规范减少安全威胁和损失。数据安全使用类安全标准，主要是与物联网通信网络和业务系统相配套的数据类安全标准，更加倾向其业务属性，一般包括数据安全等级分类、数据访问与共享规范、数据流转与应用标准等内容，此类标准通常与数据安全交换、数据传输与隐私保护类相关联，或在同一标准中体现。物联网运维管理安全标准，包括物联网安全管理、物联网安全响应、物联网安全评估、物联网安全审计、物联网安全运营等相关标准、指南或规范，涉及物联网系统安全规划、研发上线与安全部署、漏洞预警发现与修补等内容。物联网升级改造类安全标准，是指针对物联网系统进行局部改造、设备替换、技术升级、数据迁移等行为可能带来的安全风险，制定的升级改造安全评估、升级改造安全规程、数据备份与恢复等系列安全标准或指南，避免因物联网系统升级改造带来安全的不稳定性。物联网及其关联技术的快速发展，带来了物联网新技术整合应用的普遍性，这一类安全标准属于物联网与其他新兴技术的结合部分，包括新技术自身的系列安全标准，以及其与物联网联合应用带来的集成接入、数据交互、通信传输、管理控制、外部环境等系列安全内容，既可通过新立标准规范的方式也可通过现有标准制修订的方式纳入物联网安全标准体系。

本节从技术视角参考常见的物联网分层架构对物联网安全标准体系进行了描述，值得指出的是，这种分类视角仅是多种分类方法的一种，且随着 5G/6G、天基通信、边缘计算、未来网络等新 ICT 技术的融合发展[17]，物联网各项支撑技术的边界更加模糊，对应的物联网安全标准分类将会存在一定的交叠，实际安全标准也会存在跨类现象。

3 物联网安全标准化推进思考

《国家标准化发展纲要》要求，“在两化融合、新一代信息技术、大数据、区块链等应用前景广阔的技术领域，同步部署技术研发、标准研制与产业推广，加快新技术产业化步伐”[18]。尽管国际国内结合物联网安全应用需要制定颁发了系列安全标准，但依然难以适应物联网安全威胁激增对安全标准化的需要。结合物联网安全标准研究与应用现状，提出如下思考建议。

首先要牢固树立安全标准理念，加强安全一体化设计。物联网产业生态长期以来存在标准化不足、碎片化严重、功能模块复用率低、安全威胁面广等现象，其中标准理念落实不够、全流程标准化程度不足是导致这些外在表象的重要原因。安全标准作为物联网标准体系的组成部分，应与物联网其他标准一起，全流程贯穿到系统设计、应用开发与部署管理全过程，实现安全与架构、技术、功能、数据等的一体设计，避免安全标准和设计在物联网产品或系统使用时才开始考虑带来的滞后性。

其次要加强现有安全标准宣贯，提升安全标准化程度。物联网安全标准体系框架基本确立，国家和行业系列物联网安全标准陆续发布，这些为物联网安全应用提供了基础。但受种种原因影响，物联网安全标准宣传贯彻力度不够，部分物联网从业者对现有物联网安全标准的范围和内容了解不深，一些物联网项目实践者在物联网安全标准贯彻上打了折扣，从而给物联网应用带来了安全威胁。未来，应以《国家标准化发展纲要》精神为指导，优化物联网安全标准化运行机制，加大现有安全标准实施应用力度，加强物联网项目安全标准化评估，着力解决安全标准研制与应用脱节等现象，推动物联网安全标准体系高质量健康发展。

然后要优化完善安全标准体系，补齐安全标准薄弱项。安全标准体系化程度决定了物联网产业应用的安全成熟度。当前物联网安全标准体系中条码、射频识别和感知终端类标准相对较多[19]，而在网关与边缘计算安全、物联网安全管理、数据与隐私保护、物联网安全风险评估、物联网应用安全规范、物联网运维安全与安全审计等方向标准缺口较大，在新型物联网芯片与协议，北斗、5G、边缘计算、区块链、人工智能等新技术整合类方向安全标准十分薄弱。应结合物联网标准化整体布局，加大物联网安全领域薄弱标准的立项投入，强化标准之间的体系配套性，支撑物联网安全与产业发展相配套。

最后应鼓励行业领域安全标准制定，建强标准化人才队伍。物联网应用涉及诸如智能医疗、智慧交通、智能物流、智慧矿山、智能战场等众多行业和多个领域，呈现出应用样式差异大、应用链条跨度广、安全防护等级需求不一致等特点，因而对物联网安全标准需求也不尽一致。需要物联网标准化组织或机构在加大物联网通用安全标准制定的同时，应结合新兴或特殊领域应用特点，鼓励行业领域物联网安全标准制定，同步加强物联网标准化通用人才和领域专业人才队伍的培养，为物联网标准化事业提供持续发展后劲。

4 结论

随着《物联网新型基础设施建设三年行动计划(2021-2023 年)》的发布[20]，可以预见物联网将在我国经济社会和国防军事领域发挥更强的支撑和赋能作用，物联网安全是物联网产业健康发展的重要保障，物联网安全标准

将成为下一步研究和关注的焦点。

本文结合物联网发展趋势，概述了国际国内物联网安全标准化组织，从技术和应用视角对物联网安全标准进行了分类，尝试给出了物联网安全标准体系框架，并针对性提出了物联网安全标准化推进建议。下一步将结合物联网行业应用和新技术发展，深化物联网安全标准研究，加大安全标准应用推进。

参考文献

[1] 周开宇.ITU-T 物联网标准化综述[J].电信技术，2016(5)：13-15.
[2] 中国互联网发展报告[R].第二十届中国互联网大会，2021.
[3] 张玉清，周威，彭安妮.物联网安全综述[J].计算机研究与发展，2017，54(10)：2130-2143.
[4] 肖益珊，张尼，刘廉如，等.物联网安全标准及防护模型研究概述[J].信息技术与网络安全，2020，39(11)：1-7.
[5] 赵佩，陶鹏，李翀，等.物联网信息安全技术标准研究与解读[J].河北电力技术，2019，38(5)：1-3.
[6] 付敏，蒲小英，秦伟强.基于网络安全等级保护 2.0 标准的物联网安全体系架构[C]//2019 中国网络安全等级保护和关键信息基础设施保护大会论文集，2019：4.
[7] 刘巍，王冬鸽.物联网安全体系结构研究[J].物联网技术，2016，6(4)：61-63.
[8] 何艾玲，汤学军，陈卫平，等.基于三维结构模型的医疗健康物联网信息标准体系表编制方法设计与研究[J].中国标准化，2016(12)：127-131.
[9] 杨林.农业物联网标准体系框架研究[J].标准科学，2014(2)：13-16.
[10] 全国信息安全标准化技术委员会通信安全标准工作组.物联网安全标准化白皮书[R].2019-10.
[11] GB/T 33745-2017，物联网术语[S].2017.
[12] 吴晗.基于 AMQP 的消息中间件的设计和实现[D].南京：东南大学，2019.
[13] 陶伟，潘丰，崔恩隆，等.MT7628 与 OpenWrt 的 MQTT 异构协议设计[J].单片机与嵌入式系统应用，2021，21(9)：14-17，22.
[14] 雷煜卿，仝杰，张树华，等.能源互联网感知层技术标准体系研究[J].供用电，2021，38(7)：14-20，33.
[15] 宋金圣.大容量物联网网关技术研究与实现[D].成都：电子科技大学，2021.
[16] 卢周正.基于 USB 3.0 总线标准的疲劳试验机控制器设计与实现[D].杭州：浙江大学，2017.
[17] 曲至诚.天地融合低轨卫星物联网体系架构与关键技术[D].南京：南京邮电大学，2020.
[18] 中共中央、国务院.《国家标准化发展纲要》[Z].2021.
[19] 周丽莎，孔勇平，陆钢.物联网安全政策解读及技术标准综述[J].广东通信技术，2017，37(12)：39-41，45.
[20] 布轩.《物联网新型基础设施建设三年行动计划(2021-2023 年)》解读[N].人民邮电，2021-09-30(008).

(收稿日期：2021-10-27)

作者简介：

李峰(1982-)，男，博士，高级工程师，主要研究方向：物联网、智能物流。

陈亮(1991-)，男，硕士，工程师，主要研究方向：物联网。

李凯(1992-)，男，博士，工程师，主要研究方向：物联网。

扫码下载电子文档

(上接第 7 页)

challenge on action recognition for videos in the wild[J]. Computer Vision and Image Understanding，2017，155：1-23.
[28] KUEHNE H，JHUANG H，STIEFELHAGEN R，et al.Hmdb51：A large video database for human motion recognition[C]// High Performance Computing in Science and Engineering'12，2013：571-582.
[29] REDDY K K，SHAH M.Recognizing 50 human action categories of web videos[J].Machine Vision & Applications，24(5):971-981.
[30] SOOMRO K，ZAMIR A R，SHAH M.UCF101：a dataset of 101 human actions classes from videos in the wild[J].Computer Science，2012：231-243.
[31] LAPTEV I，MARSZALEK M，SCHMID C，et al.Hollywood2：human actions and scenes dataset[Z].2008：12-16.
[32] ARUNNEHRU J，CHAMUNDEESWARI G，BHARATHI S P. Human action recognition using 3D convolutional neural networks with 3D motion cuboids in surveillance videos[J]. Procedia Computer Science，2018，133：471-477.
[33] SHORE T，ANDROULAKAKI T，SKANTZE G.KTH tangrams：a dataset for research on alignment and conceptual pacts in task-oriented dialogue[C]//11th International Conference on Language Resources and Evaluation，LREC 2018，2019：768-775.
[34] YUE-HEI NG J，HAUSKNECHT M，VIJAYANARASIMHAN S，et al.Beyond short snippets：Deep networks for video classification[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition，2015：4694-4702.

(收稿日期：2021-11-29)

作者简介：

杨戈(1974-)，男，博士，副教授，主要研究方向：人工智能技术、计算机视觉技术、网络智能化技术。

邹武星(1990-)，男，硕士研究生，主要研究方向：人工智能技术、计算机视觉技术。

扫码下载电子文档

版权声明