A Survey on Standards for Interoperability and Security in the Internet of Things

Euijong Lee, Young-Duk Seo, Se-Ra Oh, and Young-Gab Kim, *Member, IEEE*

***Abstract*—Recently, there has been an increase in studies relating to the Internet of Things (IoT) in various fields, such as smart cities, smart homes, smart factories, and healthcare. In an IoT environment, several entities, including users, devices, and information resources, are interconnected and interworked with services. Therefore, interoperability between different entities is essential to accomplish the goals of IoT systems. Further, security is another important aspect to achieve in an IoT environment to protect information resources and privacy when networking between different entities. Therefore, security and interoperability may be significant barriers in the implementation of IoT in the real world. Several studies have been conducted to investigate methods for accomplishing interoperability and security in IoT, but they address only specific problems. Hence, compatibility and generality must be considered to accomplish the goals of IoT systems. International standards provide general methods by listing protocols, rules, guidelines, and characteristics that are defined and approved by authorized organizations, helping develop and manage systems efficiently by applying these standards; interoperability and security are supported by adopting standards in development and management. Therefore, the adoption of international standards is required to overcome the barriers in IoT. Furthermore, international standard organizations are developing IoT-related standards that may provide a solution to interoperability and security. However, a study focusing on interoperability- and security-related standards has not yet been conducted. Therefore, in this paper, we focus on international standards related to interoperability and security for IoT environments. Moreover, we studied international standard organizations that have been developing standards for IoT. In this study, a systematic literature review is conducted, and international standards are analyzed. In addition, any remaining challenges related to interoperability and security for IoT standards are discussed.**

***Index Terms*—Internet of Things, interoperability, security, international standard.**

I. Introduction

THE INTERNET of Things (IoT) is an important research topic and includes the study of various fields such as automobiles, smart cities, healthcare, smart homes, and smart factories. In an IoT environment, several entities such as users, devices, and information resources are interconnected with services [1]. Therefore, interoperability is essential for accomplishing interworking among different entities. In addition, interoperability must consider security-related factors to protect data and privacy and prevent malicious activities. In practice, based on the Bain & Company report [2], industrial companies in the United States (U.S.) regard interoperability as the biggest barrier to IoT adaptation, whereas in Europe, security is considered the biggest barrier. In addition, based on Gartner's reports [3], [4], interoperability and security are deemed major challenges for IoT architecture development. The reports reveal that interoperability and security must be considered to enable the implementation of IoT in the real world. Furthermore, a European consortium, including industry and academic partners, has recently been organized for IoT framework development to solve interoperability and security problems [5].

International standards in information and communication technology (ICT) fields provide guidance and protocols to help with the production and utilization of information technologies; thus, following these standards may help in implementing ICT-related systems. Therefore, it is important to reflect on the standards not only during implementation, but also during research. In IoT fields, several existing standards have been applied to implement systems such as network protocols and data formats. Furthermore, several international standard organizations (e.g., International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), the International Telecommunication Union (ITU-T), and Internet Engineering Task Force (IETF)) are participating in generating IoT-related standards, such as architecture, framework, network protocols, and definitions, and they have published various standards. In addition, the adoption of standards can support interoperability and security that are guaranteed by these standards. Several studies have applied these standards for interoperability and security in IoT; for instance, test platforms [6], [7], interoperable architectures [8]–[10],

Manuscript received April 9, 2020; revised August 26, 2020, December 11, 2020, and February 2, 2021; accepted March 16, 2021. Date of publication March 19, 2021; date of current version May 21, 2021. This work was supported in part by the Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korea Government (MSIT, Development of Artificial Intelligence Based Video Security Technology and Systems for Public Infrastructure Safety) under Grant 2019-0-00231, and in part by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIT) under Grant 2021R1A2C2012635, Grant 2021R1G1A101097111, and Grant NRF-2019R1F1A1062480. *(Corresponding author: Young-Gab Kim.)*

Euijong Lee is with the Department of Computer Science, Chungbuk National University, Cheongju 28644, South Korea (e-mail: kongjjagae@cbnu.ac.kr).

Young-Duk Seo is with the Department of Computer Engineering, Inha University, Incheon 22212, South Korea (e-mail: mysid88@inha.ac.kr).

Se-Ra Oh and Young-Gab Kim are with the Department of Computer and Information Security, and Convergence Engineering for Intelligent Drone, Sejong University, Seoul 05006, South Korea (e-mail: terious551@sju.ac.kr; alwaysgabi@sejong.ac.kr).

Digital Object Identifier 10.1109/COMST.2021.3067354

software development processes [11], protocols [12]–[15], platforms [16], [17], and semantic interoperability [18]) have been investigated for interoperability with international standards. In addition, authentication/authorization [19], networks [20], [21], protocols [22], firmware [23], and frameworks [24] have adopted international standards for IoT security. Despite the existence of considerably extensive international standards related to interoperability and security for IoT, little attention has been paid to surveying these standards. Furthermore, most survey research focused on analyzing interoperability and security-related research rather than standards [25]–[34].

In this paper, we focus on interoperability and security related international standards for IoT, and we also investigated international standard organizations that frame IoT-related standards. To conduct an effective survey on international standards, we referred to a systematic literature review (SLR) process [35]. Our primary goal was to identify international standards related to interoperability and security related concerns for the IoT. Further, we classified standards according to detailed factors of interoperability and security. Based on the survey results, a discussion and remaining challenges are presented for interoperability and security in IoT.

Contribution: The main contributions of this study are summarized as follows:

- To the best of our knowledge, this survey is the first to provide a deeper summary of IoT-related international standards for interoperability and security.
- International standards organizations and subcommittees responsible for developing IoT-related standards are investigated.
- International standards addressing interoperability and security issues in IoT are reviewed in detail.
- Challenges and future research directions related to interoperability and security standards are discussed.
- The results can facilitate the development of standard-based interoperability and security solutions in IoT environments.

The remainder of this paper is organized as follows. Section II provides background and motivation from IoT-related reports. Section III discusses survey research related to interoperability and security in IoT. The methodology used in this study is described in Section IV. Section V introduces international standards organizations, and Section VI presents international interoperability and security standards for IoT environments. In Section VII, a discussion is provided, and open challenges are presented. Section VIII concludes the paper.

II. Background and Motivation

Herein, we introduce the background and motivation for this survey. Initially, we define ICT standards and the related standards organizations. Subsequently, interoperability and security are introduced, and their importance is discussed. In addition, the motivations and research goals of this study are presented.

A. Standards and Standards Organizations

A standard can be defined as "a document defined and approved by the agreement of authorized organizations, and the document provides rules, guidelines, or characteristics for common and repeated use to achieve an optimal level within the given scope [36]". More specifically, in ICT fields, a standard can be defined as a protocol and a set of protocols that provide various information and communication services or its usage among information systems that are connected via a communication network [36]. Therefore, standards help in the production and utilization of information technology. In summary, a standard can be denoted as a predefined appointment, and standardization refers to procedures or activities that define standards. In addition, standards can be classified as de jure and de facto by organizations establishing standards. The word "de jure" means "having a right or existence as stated by law" according to the Cambridge dictionary [37]. Therefore, de jure standards are compulsory in specific topics (i.e., de jure is called an obligatory standard), and official standard organizations (e.g., ISO, IEEE, and ITU-T) produce the de jure standards. The word de facto means "existing in fact, although perhaps not intended, legal, or accepted" [37]. Therefore, de facto standards are not obligatory, but have achieved a dominant position by public acceptance or market forces. Companies, consortiums, or forums can be publishers of de facto standards. However, de facto standards are changed as de jure (e.g., HTML, PDF, and QWERT).

B. Advantages of Applying Standards

Standards provide a wide range of details, from specific aspects to conceptual information, depending upon their purpose. Specifically, some standards provide detailed specifications to guarantee accurate operations between different systems or description without information loss. For example, network protocol related standards (e.g., IEEE 802.11 [38], CoAP [39], and WebSocket [40]) provide detailed specifications to guarantee communication between a sender and receiver, and Web standards (e.g., HTML, CSS, and XML) provide formats to describe documents in Web pages. In this case, interoperable operations and security can be guaranteed if the standards are correctly applied. However, some standards provide conceptual information (e.g., software architecture, framework, and reference model), and the goals of these standards are to provide general aspects for developing software, systems, and environments. In addition, the standards are developed by experts who have experience in specific fields; thus, conceptual standards provide reasonable criteria for developing software and systems. Consequently, applying conceptual standards can help improve efficiency, reduce time, and prevent risks during development and management. It is also easy to apply recent technologies that are based on these standards. The advantages of applying standards are summarized below:

- Standards can support interoperable operations and information change without information loss by following standardized formats.
- Standards can support security that is guaranteed by them.
- Reasonable criteria are provided to develop and manage systems, frameworks, software, and environment.
- Standard can help improve the efficiency of the development processes (e.g., reducing time and preventing risks).
- Recent technologies can be applied based on these standards.

C. Interoperability and Security in IoT

The term "interoperability" is defined as "the degree to which two products, programs, etc. can be used together, or the quality of being able to be used together" according to Cambridge Dictionary [37]. In addition, in ICT, the term can be defined as "capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units" in ISO/IEC 2382:2015 [41]. Furthermore, the term "security" can be defined as "the protection of information against being stolen or used wrongly or illegally" in ICT fields [37]. Security is one of the most important factors for obtaining a secure system and environment, and lack of security can cause serious risks. Both factors are important for implementing and realizing an IoT environment. In addition, interoperability and security must be developed with consideration of each other according to the characteristics of the IoT environment, where various entities (e.g., actuators, sensors, platforms, frameworks, concepts, and users) are connected and exchange information. In this process, secure identification (e.g., authentication and authorization) is required, and interoperable identification must also be ensured so that an IoT system can be organized without information loss regarding its entities. In addition, when data are exchanged between different IoT entities, these data must be translated without information loss. To accomplish this, an interoperable data exchange protocol and a secure transport method are required. Moreover, both factors should be considered in various aspects of IoT, such as architecture and framework design, platform development, and scenario building.

D. Importance of Interoperability and Security in IoT Market

Herein, we introduce reports from an industrial perspective, indicating the importance of interoperability and security in IoT. Bain & Company [42] is an American management consulting company that provides various reports to advise public, private, and nonprofit organizations. It also provides IoT related reports, research, and surveys to the public since 2014 [43]. Its reports include impediments (e.g., security, interoperability, integration between Information Technology (IT) and Operational Technology (OT), unclear Return on Investment (ROI), technical expertise, data portability, etc.) that hinder the implementation of IoT. In a report published in 2016 [44], the company conducted a survey to investigate concerns regarding the implementation of IoT from its customers. The results indicate that security is a significant factor, and interoperability is also listed as a concern. In 2018, the company also discovered significant barriers limiting the adoption of IoT solutions [45]. In the surveyed results, security was a significant concerning factor, similar to previous reports, and interoperability as a concern ranked higher compared to previous results. According to a recent survey [46] of the same company, the concerning factors differ by region. The survey data was collected from Europe and the United States. Although security is the principal obstacle in achieving IoT in Europe, interoperability is the principal barrier in the U.S. These regions are concerned about security and interoperability for IoT adoption. In summary, from surveys conducted by Bain & Company, security is the principal concerning factor in achieving the IoT environment, and the importance of interoperability as a concern is steadily increasing.

Gartner [47] is a global research and advisory company that provides information, advice, and tools for various fields, including ICT. In their report, they have introduced the top five challenges for enterprise architecture for IoT [3], [4]: adoption ideation-based approach, business scenarios, managing risks, development of interoperability strategy, and IoT experience. However, they have emphasized that managing IoT security is important because it has a different traditional approach to security. In addition, developing an interoperability strategy is important for establishing enterprise architectures for IoT. According to a report from Gartner, interoperability and security in the IoT are required to accomplish enterprise architecture.

A European consortium has been organized on Brain-IoT [48] for the IoT framework to improve interoperability and security [5]. The consortium includes industry and academic partners (e.g., Airbus CyberSecurity, Siemens AG, and Robotnik) from different European countries, such as the United Kingdom, Spain, Germany, Italy, and France. The goal of the consortium is to focus on the framework and methodology to support IoT platforms, model-based tools for the development process, and integrated solutions for interoperability and security in IoT. In addition, the creation of the consortium shows that interoperability and security are expected to gain more importance in the future to realize IoT.

E. Motivation and Research Goals

Several studies have investigated interoperability and security problems in IoT [26]–[33], [49]–[58]. Our objective is to find interoperability and security solutions that can be applied to IoT using general methods and purposes; thus, we focus on international standards. A standard is a document that is defined and approved by authorized organizations that provide rules, guidelines, and characteristics to address specific problems. Therefore, standards can support interoperable operations between different systems, and standard-based artifacts (e.g., framework, architecture, and environment) can be conveniently interconvertible. This characteristic may help solve

interoperability problems by applying standards. Furthermore, standards can support development and management processes by providing various artifacts (e.g., framework, architecture, data format, network protocols, and use cases). Applying standards in developing and managing IoT systems can help interoperability and security problems that are guaranteed by them. Consequently, standards can be efficient sources for research related to interoperability and security, and various studies have applied international standards in various IoT fields to resolve interoperability (e.g., test platforms [6], [7], interoperable architectures [8]–[10], software development processes [11], protocols [12]–[15], platforms [16], [17], semantic interoperability [18]) and security (e.g., authentication/authorization [19], networks [20], [21], protocols [22], firmware [23], and frameworks [24]). We also intend to share with other researchers the analysis results regarding international standards related to interoperability and security. This can facilitate standard-based research. To this end, we indicate international standards organizations that have developed IoT standards and the related publications. In addition, we survey and analyze international standards related to interoperability and security for IoT environments.

III. Related Surveys

In this section, we introduce previous survey studies that analyzed interoperability and security for IoT. The survey papers related to interoperability are introduced first, followed by security-related papers. Noura *et al.* [25] provided a taxonomy of interoperability in the IoT and approaches to handle interoperability. In addition, the survey provides standard frameworks, IoT platforms, and IoT projects for interoperability. The existing proposals are categorized according to interoperability classifications, that is, gateways, virtual networks, networking technologies, open API, SOA, semantic Web technologies, and open standards. Di Martino *et al.* [26] reviewed common architecture solutions for IoT, including standardized and commercial architectures. API representations were also analyzed because common APIs may be a possible solution for interoperability between different service providers. The survey identified a set of real-case scenarios based on the architectures, and security and interoperability challenges were identified from these scenarios. However, the survey only considered the de jure standards (i.e., ISO/IEC, ITU-T, and IETF). Burzlaff *et al.* [49] focused on semantic interoperability for IoT, and in particular, they investigated ways to solve interoperability problems between applications, services, and software platforms. The results show that interoperability research is increasing with a methodical viewpoint, and that most interoperability research relies on predefined semantic standards (e.g., Semantic Sensor Network Ontology [59], W3C IoT Thing description [60], and GeoSPARQL [61]), which were reinforced for specific purposes. In addition, the survey results indicate that not only the performance but also the efficiency aspects have to be considered. Gyrard [32] reviewed and analyzed ontology-based software tools for interoperability in IoT and WoT. Kambourakis *et al.* [53] reviewed the IoT wireless personal area network (WPAN) protocol stacks, namely, Bluetooth low energy (BLE) [62], Z-Wave [63], ZigBee [64], Thread, and EnOcean. These protocols are concisely analyzed with respect to security features (such as confidentiality, message authenticity and integrity, anti-replay, man-in-the-middle attack protection, and device authentication). The studies were reviewed and divided into two parts. In the first, security features are provided for specific wireless IoT protocols, whereas in the second, a discrete comparison of the different layers of the protocol stack is provided, as well as contributions related to the security of IEEE 802.15.4 [65]–[69]. Ganzha *et al.* [55] surveyed methods and tools for supporting semantic interoperability in the INTER-IoT project, which is aimed at designing, implementing, and testing an interoperability framework among different IoT platforms [70]. Moreover, recent ontologies that were developed in IoT standards and research are provided. These ontologies are classified into general-purpose and specific use cases in INTER-IoT. One such use case is mobile and Web-based health (i.e., (e/m)Health). In (e/m)Health, medical data are collected from heterogeneous resources, and healthcare services are provided. The collected data are processed in a cloud-enabled system. The other use case is transportation and logistics. INTER-IoT focuses on the commercial perspective of transportation and logistics in a restricted domain (i.e., port logistics). Several ontologies are introduced and classified based on the purpose of the use cases. In addition, a multistep process is introduced to achieve semantic interoperability: formal representation using ontology language and applying ontology matching.

In addition to interoperability, several security-related survey papers exist for the IoT. Alaba *et al.* [27] focused on security threats and vulnerabilities, and analyzed existing research on the IoT. The survey paper provides a taxonomy of security threats and vulnerabilities in the context of different layers (i.e., application, architecture, and communication). In particular, they provided an analysis of communication technologies that can be used for IoT environments. A possible solution structure for IoT security and open research problems is also provided in the survey paper. Yang *et al.* [50] analyzed existing research studies on the classification of IoT attacks and security mechanisms as well as studies on authentication and access control in IoT. In addition, IoT security problems and solutions in four different layers were examined (i.e., perception, network, transport, and application). Ghorbani and Ahmadzadegan [28] focused on security challenges in the IoT. Their paper uses a definition of IoT based on the standards of the International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 (ISO/IEC JTC 1), ITU-T, and oneM2M; however, these standards were not analyzed but rather used to define the IoT. Security challenges are classified into implementation, privacy, network infrastructure, quality of service (QoS), security threats, object identification, authentication, authorization, light cryptography, secure protocol, vulnerability, malware, Android OS related, and security in business. Yu *et al.* [30] surveyed the security

requirements for wireless sensor networks (WSNs), which are the basic elements of IoT networks; however, although the survey provided general security requirements, network-related international standards were not considered (e.g., protocols). Oracevic *et al.* [31] defined characteristics for secure IoTs, and the characteristics consisted of three categories: confidentiality, integrity, and authentication. In addition, security problems are categorized into different layers (i.e., application, transport, and sensing). Based on these characteristics and security problems, previous studies were surveyed for solutions to achieving security with related secure requirements. Mena *et al.* [29] surveyed IoT security and privacy challenges from technological and architectural viewpoints. They focused on intrinsic vulnerabilities and implications related to security challenges, including confidentiality, integrity, and availability. The available protocols and technologies were analyzed, and related studies were classified. Lin *et al.* [33] conducted a comprehensive overview of IoTs, including system architecture, enabling technologies, security and privacy problems, and integration of fog/edge computing and its applications. In the security-related analysis, security features of IoT are presented (i.e., confidentiality, integrity, availability, identification, authentication, privacy, and trust) as well as security challenges in several layers (i.e., perception, network, and application layer). Hossain *et al.* [52] conducted a detailed analysis of security-related problems in IoT environments and discussed security-related constraints, requirements, and vulnerabilities. The security constraints were classified as limitations based on hardware, software, and networking. Furthermore, the security requirements were classified according to whether they were related to information, access-level, and functional security. Finally, a list of security vulnerabilities and attacks was provided, and general research directions were proposed. Qui *et al.* [54] provided theoretical, methodological, and technical guidance for IoT access control. The requirements were analyzed based on the characteristics of the IoT search and were classified into two categories: access-control policy composition and authoring. In the policy combination requirement, policy description methods (e.g., common policy language, extensible access-control markup language, and security-assertion markup language) were introduced, and a combination of policies and models was investigated. In addition, conflict detection and resolution were considered in the access-control policy composition requirements. Moreover, in access authorization, attribute discovery mechanisms, policy mining, and authorization models were analyzed. Finally, open problems related to access control for IoT were discussed. Hou *et al.* [56] investigated IoT security from a data perspective and proposed a three-level approach to analyzing IoT security: one-stop, multi-stop, and end-application. At the one-stop level, IoT security in the end device was considered; thus, data were collected, transmitted, and received from the end device. In addition, several security-related aspects, including confidentiality, authenticity, data security, and data safety, were considered. At the multi-stop level, data were used among a group of IoT entities; thus, secure communication, authentication, and access control were investigated. At the end-application level, data used in IoT applications are spanned; thus, the results included privacy concerns, forensic challenges, social challenges, and legal challenges. Hassija *et al.* [57] focused on security threats and challenges in several IoT application areas. Security threats were classified into four layers in an IoT system (i.e., sensor, network, middleware, and application), and the requirements for secure IoT applications were discussed. In addition, new technologies (i.e., blockchain, fog computing, edge computing, and machine learning) were applied to enhance IoT security. Neshenko [58] analyzed IoT vulnerabilities and provided a detailed taxonomy including layers, security impact, attacks, countermeasures, and situational awareness capabilities. Furthermore, challenges and initiatives for improving IoT security to address vulnerability problems were considered.

Moreover, some surveys focused on interoperability and security in IoT. Elkhodr *et al.* [51] discussed interoperability, security, management, and privacy problems. Regarding interoperability problems, the concept of integration between WSNs and IoT was introduced in the following types: network-based, independent, and hybrid. In addition, other interoperability challenges (i.e., thing interaction, virtual representation of things, searching and accessing things, and syntactic interoperability between things) were introduced. The correspondence between interoperability and security was explained. In addition, security-related challenges resulting from Internet security problems (i.e., end-to-end security, data security, identity and access management, compliance, access control, physical risk, and DoS risk), and newly emerged security and privacy-related challenges in IoT were presented. Moreover, IoT management-related problems and challenges were presented (configuration management, things control, monitoring, things maintenance, things performance, things security and privacy, and energy management). However, the focus was primarily on specific challenges, and although the importance of standardization was emphasized, problems related to standards were not considered.

Several surveys on IoT interoperability and security have been published. However, most of them are concerned with existing security and interoperability technologies, and surveys exploring interoperability and security standards are rather scarce. Although Hwang and Kim [34] surveyed IoT security standards, they only mentioned a standards organization and provided a list of security-related international standards; thus, there was no detailed analysis. The present study focuses on international standards organizations for IoT and international interoperability and security standards. Table I shows a comparison of existing surveys on interoperability and security in IoT.

IV. Methodology for Survey

A. Overview

We performed a systematic literature review based on Kitchenham's guideline [35] to identify relevant international standards for interoperability and security in IoT. Fig. 1 denotes the procedure of the literature review.

TABLE I
COMPARISON OF RELATED RESEARCH

Survey	Description/goal	Related research topic		Survey source					
		Interoperability	Security	IoT platforms	Research	Tool	Standard	Commercial research	Internet
Elkhodr et al. (2016) [51]	A survey that identifies interoperability, management, security, and privacy problems in IoT.	✓	✓		✓				
F. A. Alaba et. al. (2017) [27]	It provides information on IoT security threats and vulnerabilities by conducting an extensive survey of existing studies on IoT security.		✓		✓				
Fabian et al. (2019) [49]	A study on how IoT-systems engineering processes can be supported to achieve semantic interoperability between applications, services, and software platforms.	✓			✓				
Ghorbani and Ahmazadegan (2017) [28]	A survey of security challenges in IoT.		✓		✓		✓		
Gyrard et al. (2018) [32]	Review and analysis of ontology-based software tools for semantic interoperability in IoT and WoT.	✓			✓	✓			
Hassija et al. (2019) [57]	A discussion of security threats and solutions in IoT application areas.		✓		✓				
Hossain et al. (2015) [52]	It IoT analyzes attacks, surfaces, threat models, security problems, security-related requirements, and forensics.		✓		✓				
Hou et al. (2019) [56]	A survey of security technologies for IoT from a data perspective.		✓		✓				
Hwang and Kim (2017) [34]	An analysis of security standards for IoT.		✓				✓		
Jie et al. (2017) [33]	An overview of IoTs in terms of system architecture, enabling technologies, security, privacy, and integration with fog/edge computing.		✓		✓				
Kambourakis et al. (2020) [53]	A review concerned with security aspects protocol and literature investigating security weaknesses of WPANs.		✓		✓		✓		
Mahda et al. (2019) [25]	A comprehensive survey on solutions for facilitating interoperability between IoT platforms.	✓		✓					
Maria et al. (2017) [55]	Methods and tools for supporting semantic interoperability in IoT, particularly the INTER-IoT project.	✓		✓	✓	✓	✓		
Martino et al. (2018) [26]	A review of the most common architectural solutions available to develop an IoT system from a standardized to a commercial architecture.	✓	✓		✓		✓	✓	
Mendez et al. (2018) [29]	A survey on IoT security and privacy challenges from a technological and architectural perspective.		✓		✓		✓		
Neshenko et al. (2019) [58]	A survey of IoT vulnerabilities.		✓		✓				✓
Oracevic et al. (2017) [31]	It provides information on security problems, solutions, and challenges in IoT.		✓		✓				
Qui et al. (2020) [54]	A survey that provides theoretical, methodological, and technical guidance for access control in IoT.		✓		✓				
Yang et al. (2017) [50]	A survey on security and privacy problems in IoT applications and systems, with a focus on the analysis of possible solutions.		✓		✓				
Yu et al. (2020) [30]	Security requirements for wireless sensor networks.		✓		✓				
This paper	**A survey of international standards organizations for IoT, and analysis of interoperability and security-related standards in IoT.**	✓	✓				✓		

First, we started our research with the following question: "What are the current international standards for solving interoperability and security problems in IoT?" This question led us to raise the following questions:

- RQ #1: Which international standards organizations develop IoT-related standards?
- RQ #2: Which published international standards can address interoperability problems in IoT?
- RQ #3: Which published international standards can address security problems in IoT?

Deriving insights from these questions, we selected search keywords such as "security", "interoperability," and "Internet of Things / IoT". These keywords were chosen to be broad for a comprehensive search to prevent the omission of standards. Based on these keywords, we compiled standards from the international standard library (i.e., ISO/IEC JTC 1, IEEE library, ITU-T, IETF, oneM2M, and Open Connectivity Foundation (OCF)), and 104 internal standards were obtained. The selected standard organizations have actively produced IoT standards in recent years. To select standards, the following criteria were considered, and details are provided in Section IV-B. After selection, we reviewed each standard to assess whether they contained interoperability and security factors. In addition, we identified international standard organizations that focused on IoT standardization addressing interoperability and security. The details of the survey process are described in Section IV-B.

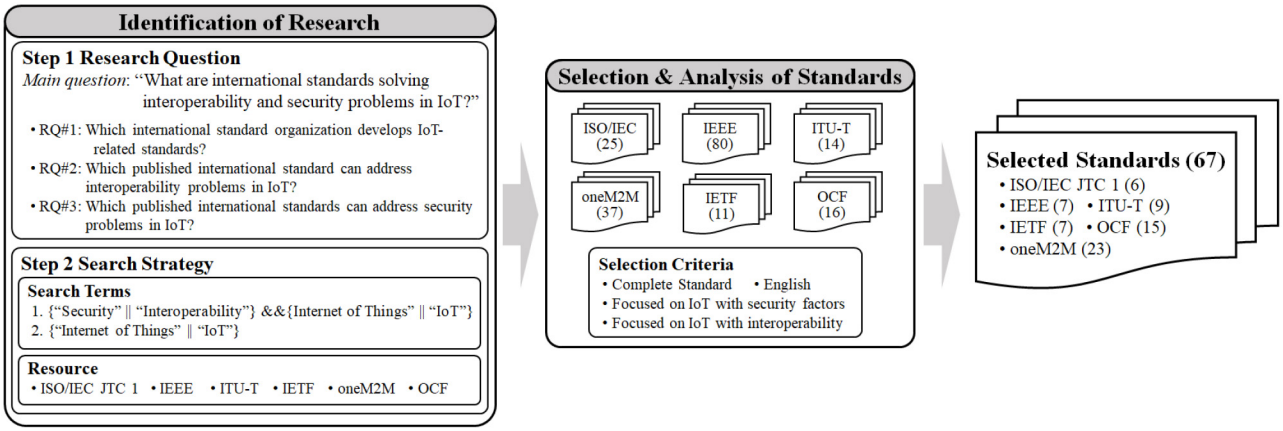

Fig. 1. Summary of procedure used for the literature review to select relevant internal standards.

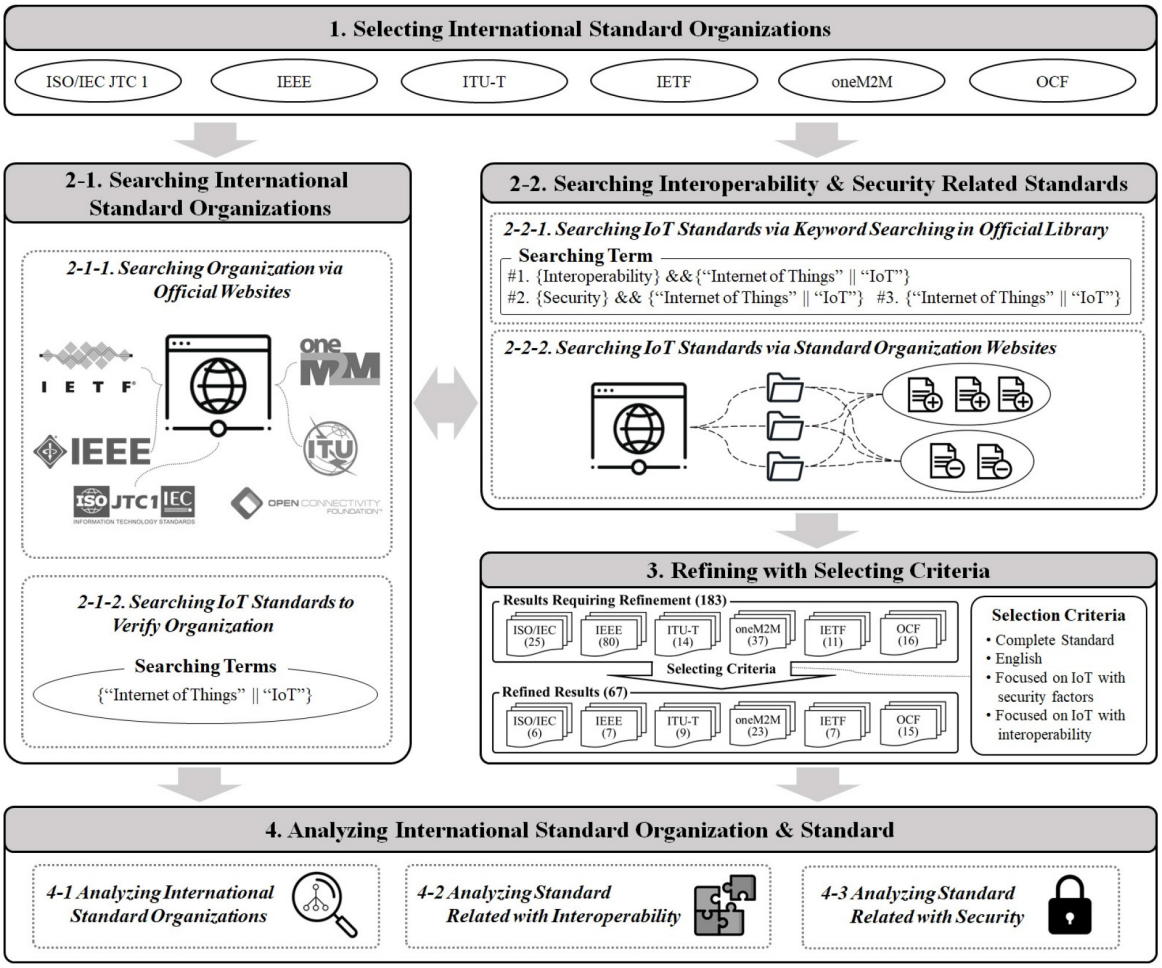

Fig. 2. Detailed process of survey.

B. Survey Process

A schematic of the systematic literature review is shown in Fig. 2. It consists of four processes. Initially, we investigated international standards organizations that have developed IoT-related standards (i.e., process #1 in Fig. 2). Thereafter, we selected three de jure international standards organizations (i.e., ISO/IEC JTC 1, IEEE standard association, and ITU-T) and three de facto international standards organizations (i.e., IETF, oneM2M, and OCF). The selected organizations actively develop IoT-related standards and provide them in document form using a systemic management system.

After the selection, departments (e.g., subcommittees and working groups) of the international standard organizations were searched, and interoperability and security-related international standards were concurrently searched for (i.e., processes #2-1 and #2-2 in Fig. 2). Both processes are complementary. The organization search can facilitate the standards search and vice versa. That is, we identified some departments

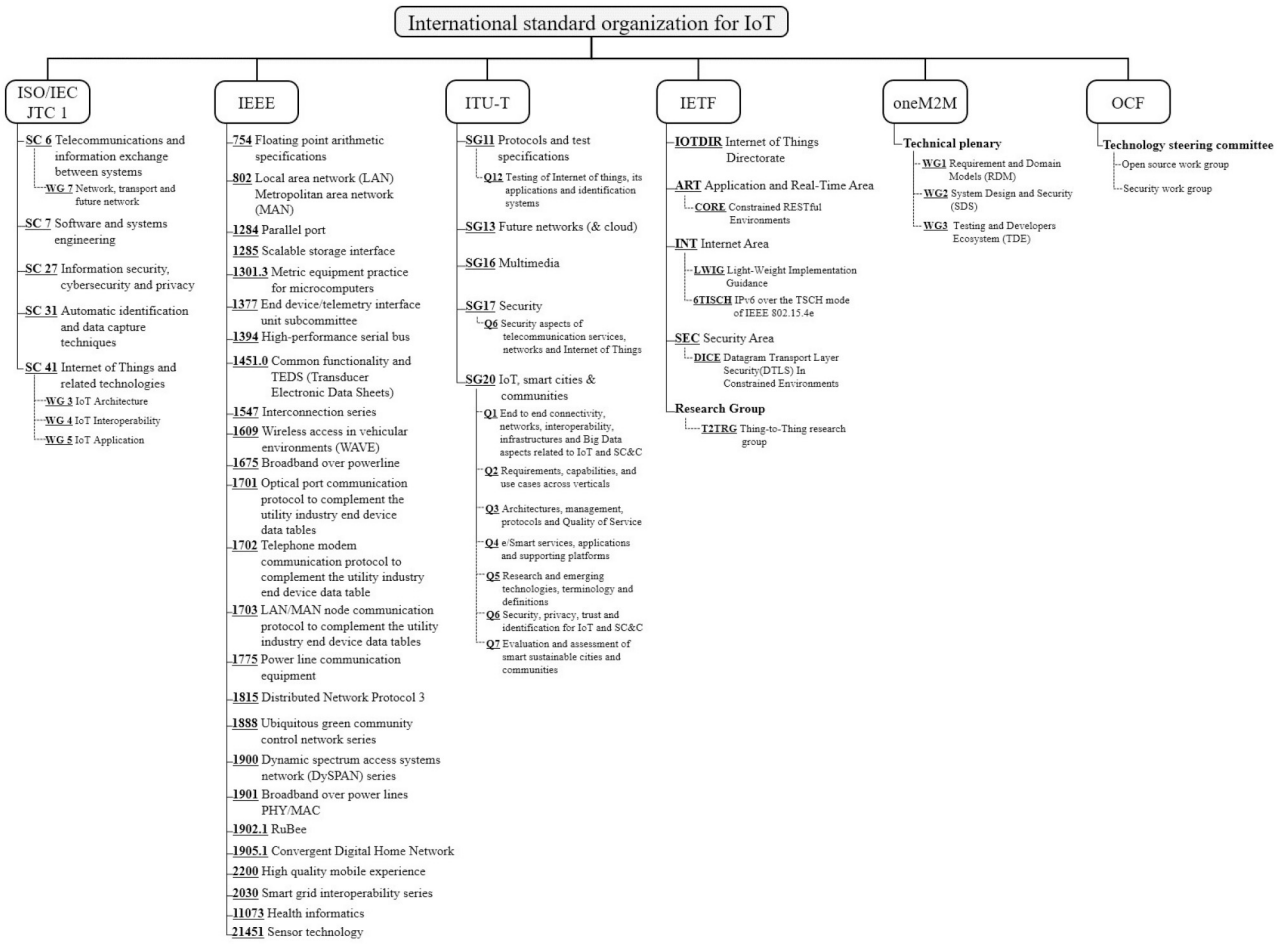

Fig. 3. Taxonomy of international standards for IoT.

of the organizations when we searched for standards, and some standards were discovered when we investigated the departments. In the latter case, we searched for organization branches by investigating official websites, and if official departments were defined to develop IoT-related standards, we added those departments as candidates for analysis. We also searched for specific terms (i.e., Internet of Things and IoT) on official websites to determine departments that indirectly develop IoT standards and added them as analysis candidates. The candidates were then analyzed in the final process (i.e., process #4-1 in Fig. 2). In addition, the standards developed in the selected departments were used as candidate standards for analysis (i.e., process #2-2-2 in Fig. 2). In addition, we searched for standards in official libraries [71]–[76] (to determine the standards of each organization). The search results were also added as candidate standards for the analysis. (i.e., process #3 in Fig. 2). For the search, the following three groups of terms are used:

- Interoperability with IoT and the Internet of Things
- Security of IoT and Internet of Things
- IoT and Internet of Things

According to the search results, 183 standards were considered candidates, and from these, 67 were selected based on the following criteria (i.e., process #3 in Fig. 2):

- Complete and maintained standards were selected. That is, standards related to development procedures (e.g., new projects, draft international standards, or final texts of international standards) and withdrawn standards were ignored. It should be noted that most standards organizations did not provide details on standards under development. Additionally, some organizations provide standards in progress, but only for information purposes.
- Publication date was not considered because international standards are constantly updated to indicate changes in technology, and they are withdrawn if they are not useful. (i.e., even if a standard is not recent, it is useful unless it has not been withdrawn).
- The leading international language is English. Hence, standards in other languages were excluded.
- Standards that can be retrieved using ISO store [71], IEEE Explore [72], ITU-T standardization [73], oneM2M [74], IETF standards [75], or OCF standards [76] were selected.
- Standards that contain interoperability factors in an IoT environment were selected.
- Standards that contain security factors in an IoT environment were selected.

Finally, search results that include the standards organizations and IoT standards for interoperability and security were analyzed (i.e., process #4 in Fig. 2). Although we considered standards that are related only to interoperability and security in IoT, the analysis of the organizations was not limited to interoperability- and security-related topics. In addition, we carefully observed the relationships among different standards. The identified international standards organizations are described in Section V. The results of the analysis for interoperability and security-related standards are presented in Section VI.

V. Standards Organizations

In this section, we introduce standards organizations that frame IoT standards; further, we describe their standardization works. Fig. 3 shows the standards organizations and organograms for IoT standardization. In ISO/IEC, we indicated the subcommittees (SC) that develop IoT-related standards. We denoted them as working groups (WG) if there are WGs focusing on a specific topic in the IoT. Several committees exist in IEEE for IoT standardization, and we organized the taxonomy with a representative number of standards committees; for example, the number of "802" denotes the LAN/MAN standard committee, and there are several networking-related standards in the 802 series. The ITU-T standard organization consists of a technical study group (SG) with questions (Q). Each SG carried out standardization work in different fields, and questions denote specific topics that have been standardized in SGs. IETF uses abbreviations for the naming of WGs. WGs also consisted of active WGs with an abbreviated name. The technical plenary of oneM2M is in charge of standardization, and there are only three WGs, that is, requirements and domain models (RDM), system design and security (SDS), and WG3, which is the Testing and Developers Ecosystem (TDE). The technology steering committee is responsible for standardization in OCF, and the open-source and security workgroups develop standards.

In the remainder of this section, international standards organizations and their work for IoT are introduced. Sections V-A, V-B, and V-C describe de jure standard organizations (i.e., ISO/IEC JTC, IEEE, and ITU-T). Sections V-D, V-E, and V-F describe de facto standard organizations (i.e., IETF, oneM2M, and OFC) and their works.

A. International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 (ISO/IEC JTC 1)

The International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 (ISO/IEC JTC 1) is the first joint international standards organization of ISO and IEC for information technology. ISO/IEC JTC 1 was established in 1987 to avoid a collision of standards between ISO and IEC [77]. In JCT 1, SC 41 was established in 2016 for the IoT, and the SC focused on industrial IoT, real-time IoT, edge computing, sensor network, trustworthiness, requirements, and wearables. Twenty-one standards have been published, and 19 work programs are in progress. Furthermore, not only SC 41, but also several other SCs and WGs determine standards for IoT. SC 31 works on automatic identification and data capture techniques and has an IoT project for unique identification (i.e., 29161:2016 [78]). SC 27 (information security, cybersecurity, and privacy protection) has under development standards related to security (i.e., 27030 [79], guidelines for security and privacy in the Internet of Things). SG 6 (telecommunications and information exchange between systems) published a standard that describes the network of everything (i.e., TR 29181-9:2017 [80], Information technology—Future Network—Problem statement and requirements—Part 9: Networking of everything). The network standard describes the general characteristics of the network of everything, including the IoT. SC 7 (software and systems engineering) has a standard for an architecture evaluation framework (i.e., ISO/IEC/IEEE 42030:2019 [81]), including IoT architecture. Furthermore, interoperability and security-related standards from ISO/IEC JCT 1 are described in Section VI-A.

B. Institute of Electrical and Electronics Engineers Standard Association (IEEE-SA)

IEEE is an institute for electronic and electrical engineering, and it has built an association for standardization called IEEE-SA [82]. IEEE-SA is a de jure standard organization that develops global standards for various electronic and electrical engineering fields, including ICT fields (e.g., software and system engineering, wired and wireless communications, healthcare IT, smart grids, computer technology, etc.)

IEEE-SA established a working group IEEE P2413 for IoT standards, whereas P2413 focused on the standards for an architectural framework for IoT. The architectural framework describes various IoT domain abstractions and the identification of commonalities between different IoT domains [83]. In addition, IEEE-SA listed 80 standards related to IoT on their website [84]. The standards can be classified into network, data type, interface, electric power management, wireless access in vehicular environments (WAVE), definition of terminology, and hearth informatics. In particular, IEEE-SA has the following network-related standards for IoT that are widely used: Wi-Fi (IEEE 802.11), ZigBee (IEEE 802.15.4), RFID (IEEE 21451-7), and WiMAX (IEEE 802.16). IEEE P1901 actively works to make standards for broadband over-power line networks for the enhancement of IoT applications. In addition, IEEE-SA listed its 46 standards that are in development related to IoT [85], and the developing standards consist of several topics, including interoperability, network, interface, security, WAVE, and smart grid.

C. International Telecommunication Union (ITU-T)

The International Telecommunication Union (ITU) is a specialized agency of the United Nations for information and communication technologies since 1865 [86]. ITU comprises three sectors: radio communication (ITU-R), development

(ITU-D), and standardization (ITU-T). As the standardization sector, ITU-T assembles experts and develops international standards. The normative standards are called ITU-T recommendations; however, the recommendations have a non-mandatory status until they are adopted into national laws [73]. ITU-T also publishes technical papers and technical reports that contain non-normative information on various topics. In addition, ITU-T publishes ITU-T handbooks for several ICT topics (i.e., operation, network planning, quality of service, implementation guide, outside plant, protection against electromagnetic effects, measurement methods, security, mobile systems, and formal languages).

The ITU-T comprises 11 study groups for standardization in various ICT fields (i.e., SG2 operational aspects, SG3 economic and policy problems, SG5 environment and circular economy, SG9 broadband cable and TV, SG11 protocols and test specifications, SG12 performance, QoS and QoE, SG13 future networks (& cloud), SG15 transport, access and home, SG16 multimedia, SG 17 security, SG20 IoT, smart cities, and communities). In particular, SG20 works for the standardization of IoT technologies, including end-to-end architectures for IoT, a mechanism for interoperability of IoT applications, machine-to-machine communication, and ubiquitous sensor networks. In addition, there are several study groups for IoT standardization in ITU-T. SG 11 is responsible for signaling requirements, protocols, and test specifications. SG 11 works for the standardization of the development of test specifications to solve global interoperability testing, covering technical means, services, QoS, and testing parameters, and they also focused on the IoT environment. SG 13 produces standards for next-generation networks, and they work to cover the network aspect of IoT. Additionally, they focus on ensuring support for IoT across future networks through cloud computing. SG 16 develops standards for multimedia coding, systems, and applications for various ITU-SGs, including the IoT. In addition, SG 17 is a study group for security, and they also focus on the security of applications and services for IoT as a secure view.

D. Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is an open international community for enhancing the Internet, and they promote voluntary Internet standards including automated network management, IoT, new transport technologies, security, and privacy [87]. In IETF, there are over 100 active working groups, and several working groups of IETF develop protocols for IoT. In particular, the IETF established an advisory group called the Internet of Things Directorate (IOTDIR) on Oct. 2014 [88], and the directorate actively works on IoT standardization. The IETF classified their standards according to maturity levels, namely, proposed and Internet standards [89]. The proposed standard is defined as "a specification that is generally stable, has resolved known design choices, is believed to be well understood, has received significant community review, and appears to enjoy enough community interest to be considered valuable. However, further experiences might result in a change or even retraction of the specification before it advances." [90]. The Internet standard is defined as follows: "An Internet Standard is characterized by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides significant benefit to the Internet community" [89], [90]. IETF also provides documents that are not standards but include useful information for Internet standardization and research. The nonstandard specification can be classified into three types: informational, experimental, and historic. The informational specification is defined as "a specification that is published for the general information of the Internet community and does not represent an Internet community consensus or recommendation" [90]. The experimental specification denotes that "a specification is part of some research or development effort" [90]. The historic specification is defined as "a specification that has been superseded by a more recent specification or is for any other reason considered to be obsolete" [90]. However, IETF assigns a number to a specification before it reaches the status of an Internet standard in the STD series, and all other specifications, including the proposed standard and nonstandard, are assigned RFC numbers.

IETF has a research group called the Internet Research Task Force (IRTF), and the IRTF organizes annual workshops for applied networking research with the Association for Computing Machinery (ACM). IRTF has 14 active sub-study groups for various Internet-related research problems, including protocols, applications, architecture, and technology [91]. The sub-study groups are focused on each topic, e.g., crypto forum, computing in the network, decentralized Internet infrastructure, global access to the Internet for all, human rights protocol considerations, Internet congestion control, information-centric networking, measurement and analysis for protocols, network management, coding for efficient network communications, path aware networking, privacy enhancements, and assessments, quantum Internet proposal, and Thing-to-Thing. In particular, the Thing-to-Thing Research Group (T2YRG) investigates open research problems related to the IoT [92] and focuses on adaptation layers connecting to IP and application layers with architectures and API.

E. oneM2M

oneM2M is a global partnership for the standardization of machine-to-machine (M2M) and IoT since 2012, and the partnership was founded by eight ICT standard development organizations (i.e., Association of Radio Industries and Businesses (ARIB / Japan), Alliance for Telecommunications Industry Solutions (ATIS / United States), China Communications Standards Association (CCSA / China), European Telecommunications Standards Institute (ETSI / Europe), Telecommunications Industry Association (TIA / United States), Telecommunications Standards Development Society (TSDSI / India), Telecommunications Technology Association (TTA / Republic or Korea),

and Telecommunications Technology Committee (TTC / Japan) [74]. Currently, oneM2M has nearly 200 participating partners and members. In oneM2M, technical plenary (TP) is responsible for conducting oneM2M technical specifications and technical reports for market requirements, and there are three working groups classified by different topics. The first WG works for the requirements and domain models (RDM), and WG 2 is responsible for System Design and Security (SDS). Finally, WG 3 works on the Testing and Developers Ecosystem (TDE).

oneM2M prepares, approves, and maintains technical specifications (i.e., standards) and technical reports for several M2M and IoT market requirements, including interoperability and security. oneM2M has released several specifications and technical reports five times. The first and second releases were updated during the third release, and the third release was ratified by oneM2M TP in December 2018 [93]. However, the fourth and fifth released drafts are provided only for the purpose of providing information because the drafts need to be changed before formal publication.

F. Open Connectivity Foundation (OCF)

The Open Connectivity Foundation (OCF) is an industry organization that develops de facto standards for interoperability in IoT ecosystems, and several telecommunication companies and device makers are participating in OCF standardization. The organization mainly focuses on two topics [64]: one is supporting manufacturers with the provision of materials (i.e., specification, code, and certified program) for interoperability with IoT devices and legacy systems, and the other is to enhance the users experience with OCF compliant devices.

OCF developed specifications (i.e., standards) for certification and interoperability. The specifications can be classified into five types: framework-related, security-related, bridging, resource-related, and onboarding. However, several ISO/IEC JCT 1 standards are based on OCF specifications; the ISO/IEC 30118 series is based on OCF specifications. Details of the relationship between ISO/IEC standards and OCF specifications are described in Section V-F. In addition, OCF sponsored an open-source project called IoTivity [94] to promote interoperability guidelines and certification programs for IoT.

VI. Interoperability and Security Standards for IoT

In this section, international standards that contain interoperability and security clauses for the IoT are described. The standards were classified by the publisher. We searched three de jure standard organizations (i.e., ISO/IEC JTC 1, IEEE-SA, and ITU-T) and three de facto organizations (OCF, IETF, and oneM2M). In addition, to categorize interoperability and security standards, we selected certain factors by considering IoT characteristics. The related definitions in ICT can be applied in IoT without change, but the characteristics of the latter should be considered. In addition, various interoperability and security factors are also considered to support the implementation and application of IoT. It should be noted that a standard can be related to different factors, thus covering various issues. We first introduce interoperability-related factors. The details are described below.

- Architecture: This includes several aspects, such as the instruction set of the architecture design, logic design, and implementation, in the description of a specific computer system [41]. Therefore, this factor considers several aspects in the design of IoT systems (e.g., wireless access in vehicular environments, Web of things, and general IoT systems).
- Behavioral: Behavioral interoperability is a related outcome from results after the exchange of information matches to prevent misuse of entities in IoT systems [95].
- Definition: This provide a set of terms and definitions to prevent misused terminology in IoT documents.
- Framework: The framework factor provides a standard way to develop and implement a general and specific IoT system.
- Identifier: In an IoT environment, several different entities can be created and used; thus, an identifier is required to distinguish them. Accordingly, related standards provide rules, methods, requirements, etc., to generate the identifier.
- Interworking: Different IoT service layers and platforms require interworking processes to accomplish the goals of the system and meet user requirements. Some standards provide specific processes to interwork with other platforms.
- Policy: Two or more systems can be interoperated in an IoT environment, and this may require legal, organizational, and policy-related interoperability. Policy-related standards concern these types of policy issues.
- Reference model: Standards that include a reference model provide an abstracted framework for understanding significant relationships between various entities of an IoT environment.
- Requirement: Several requirements should be met to establish an IoT environment with different aspects. This factor pertains to standards that contain various IoT-related requirements.
- Semantic: After information is exchanged between different IoT entities, this information should be properly interpreted. Thus, semantically related standards provide methods, rules, or protocols for lossless exchange of information.
- Syntactic: This factor is also required for information exchange, but it focuses on syntax; for example, format and rules.
- Transport: This factor is related to communication infrastructure so that data can be exchanged between different entities. Therefore, several network-related aspects are included in these factors, such as network protocols and protocol binding.
- Use case: There are various IoT environments (e.g., transport infrastructure, smart homes, public buildings, health care, and vehicles), and each environment has different needs, requirements, and considerations. To

provide information from various IoT environments to users, service providers, and developers, several standards describe use cases.

Security can cover various areas such as information, the Internet, devices, and networks, and security in ICT can be accomplished using a variety of methods. Therefore, we broadly categorized the security-related factors for IoT as follows.

- Architecture: Unlike the general concept of architecture in ICT, this factor considers security architecture to protect an IoT system. Therefore, an architecture is provided as a high-level overview of IoT security.
- Data protection: Data protection is important in IoT environments because various types of data are transferred in these environments including privacy, critical information, and commands for actuators (e.g., patient records in a hospital system, information on vehicles, and personal information in a smart home). This factor involves various IoT data protection methods, including authenticity, confidentiality, replay protection, encryption, and key cryptography.
- Framework: This factor provides standard processes for developing and implementing IoT systems with security-related issues.
- General (consideration): Several international standards include general problems and considerations related to various security issues. This factor pertains to standards providing general implementation and application information.
- Network: Networks between IoT entities are important for realizing IoT environments. From a security perspective, the network factor is related to secure transport issues. However, we regarded the network protocol as a different factor; thus, the protocol factor includes network-protocol-related standards.
- Policy: This factor pertains to security-related legal, organizational, and policy-related standards.
- Privacy: Privacy-related standards provide various aspects and information regarding different topics that constitute the main content of the standards (e.g., network protocol, use case, and platform).
- Protocol: Network-protocol-related standards that provide secure transport are related to this factor. In addition, some standards include security-related considerations to use specific network protocols.
- Secure access: This factor pertains to authentication, authorization, and access control for specific IoT domains, network protocols, and platforms.
- Use case: Several standards provide use cases for various IoT environments with security-related issues.

We tried to search for and select standards that include interoperability and security factors for IoT, but we also selected standards including one topic for both. Table II shows the summarized results of the interoperability-related standards. In addition, Table III indicates an overview of security-related standards. Furthermore, the interoperability table has a column that describes security factors related to each standard, and vice versa. Additionally, the limitations of the standards are described in the table: "domain- or platform-specific," "conceptual," "low accessibility," "market gap," and "lack of developer support." The detailed limitations of each standard are described in the remainder of this section, and the overall limitations are presented in Section VII.

A. ISO/IEC JTC 1 Standards

ISO/IEC 21823-1:2019 [95] focused on an overview of interoperability for IoT systems and a framework for interoperability within IoT systems. Thus, ISO/IEC 21823-1:2019 provides several elements and characteristics for IoT interoperability. The standard provides a facet model for interoperability, and the model is classified into five facets: transport, syntactic, semantic, behavioral, and policy. The transport interoperability facet is the commonality for communication infrastructure to exchange data between IoT entities. Several wire and wireless protocols (e.g., Ethernet, Wi-Fi, TCP/IP, HTTP/S, and MQTT) are examples of transport interoperability. The entities can be physical or nonphysical, with a distinct existence [1]. In addition, a facet includes a physical medium and transport mechanism. Syntactic interoperability is the ability to exchange information based on syntaxes (i.e., formats, rules, etc.). Web Ontology Language (OWL), Resource Description Framework Schema (RDFS), Unified Modeling Language (UML), JavaScript Object Notation (JSON), and eXtensible Markup Language (XML) can be a syntax for information exchange for syntactic interoperability. Semantic interoperability is the ability to understand the meaning of the data model within several contexts of a subject area when information is exchanged. Behavioral interoperability is related to the result of the use of exchanged information for an expected outcome. To accomplish the behavioral facet, the interface and input/out interface are described for each IoT entity, and the expected results of each operation, such as preconditions, post-conditions, and sequences of operations, also need to be described. The policy of interoperability is related to legal, organizational, and policy frameworks for the participating systems that are interoperating between IoT systems. Therefore, the facet considers government laws and regulations, IoT user policies, IoT system providers, and organization policies. The standards indicate that accomplishing all facets is recommended if it is possible for IoT interoperability, but satisfying all facets is not mandatory. However, behavioral interoperability is important for enabling interoperability among systems because a lack of behavioral interoperability can cause a significant barrier between systems. Furthermore, ISO/IEC 21823-1 describes the interoperability requirements for IoT characteristics, focusing on semantic, behavioral, and policy facets: network communication and self-description. The network communication characteristic is mainly focused on the transport facet, and the characteristic includes the physical medium and transport protocol necessary to interoperate between IoT entities. Self-description is mainly focused on the syntactic facet, and the self-description needs to describe the

TABLE II
OVERVIEW OF INTEROPERABILITY-RELATED INTERNATIONAL STANDARDS FOR IOT

Standard Name	Interoperability related factors															Limitation					Security related factors	Domain
	Use case	Interworking	Framework	Architecture	Reference model	Requirement	Definition	Syntatic	Sementic	Behavioural	Identifier	Policy	Transport	Protocol	Protocol binding	Platform specificed	Conceptual	Low accessibility	Market gap	Lack of developer support		
IEEE 1609.0 (WAVE) (2019)				✓														✓		✓	DP, GE	WAVE
IEEE 1609.11 (2010)														✓				✓		✓	SA	WAVE
IEEE 1609.12 (2019)											✓							✓		✓		WAVE
IEEE 1609.3 (2016)														✓				✓		✓		WAVE
IEEE 802.11 (Wi-FI) (2016)														✓				✓		✓	NET, PT, PR, SA	Wi-FI
IEEE 802.15.4 (WPAN) (2011)														✓				✓		✓	DP	WPAN
IETF RFC 7925 (2016)														✓			✓			✓	GE, PT	CoAP
IETF RFC 8323 (2018)														✓						✓	GE, PT	CoAP
ISO/IEC 18000 series (RFID) (2015)														✓				✓		✓	See ISO/IEC 20248	RFID
ISO/IEC 20922:2016 (MQTT) (2016)								✓	✓	✓				✓					✓		GE, PT, PR, SA	MQTT
ISO/IEC 20924:2018 (2018)							✓										✓	✓		✓		
ISO/IEC 21823-1:2019 (2019)			✓					✓	✓	✓		✓	✓				✓	✓		✓		
ISO/IEC TR22417:2017 (2017)	✓																✓	✓		✓	GE, NET, PR, UC	
ITU-T X.675 (2015)			✓								✓									✓	GE	Object identifies
ITU-T Y.2060 (2012)					✓												✓			✓	GE	
ITU-T Y.2063 (2012)			✓	✓		✓											✓			✓	GE	WoT
ITU-T Y.2066 (2014)	✓					✓											✓			✓	GE	Common IoT
ITU-T Y.4101/Y2067 (2017)						✓											✓			✓	GE	Gateway of IoT
ITU-T Y.4111/Y2076 (2016)			✓		✓	✓			✓								✓			✓	GE	
ITU-T Y.4112/Y2077 (2016)						✓											✓			✓	GE	PnP
ITU-T Y.4553 (2016)						✓											✓			✓	GE	SPSN
ITU-T Y.4702 (2016)						✓											✓			✓	GE	Device management
OCF Core Specifiation (30118-1:2018) (2019)			✓	✓				✓	✓				✓		✓	✓					FR	
OCF Security Specification (OCF-Sec) (2019)																✓					DP, FR, GE, NET, PR, PT, SA	
oneM2M TR-0001-V3.1.1 (2019)	✓					✓										✓					GE	
oneM2M TR-0010-V3.0.1 (2019)															✓	✓					GE	oneM2M and MQTT
oneM2M TR-0018-V2.5.1 (2019)	✓					✓										✓					GE	
oneM2M TS-0004-V3.15.0 (2020)														✓	✓	✓					GE	
oneM2M TS-0006-V3.6.2 (2019)														✓	✓	✓						oneM2M and CWMP
oneM2M TS-0008-V.3.5.0 (2019)															✓	✓						oneM2M and CoAP
oneM2M TS-0009-V3.5.0 (2019)															✓	✓					GE	oneM2M and HTTP
oneM2M TS-0012-V3.7.3 (2019)								✓	✓							✓						oneM2M and OWL
oneM2M TS-0020-V3.0.1 (2019)															✓	✓					GE	oneM2M and WebSocket
oneM2M TS-0023-V3.7.3 (2019)									✓							✓						Home application
oneM2M TS-0024-V3.2.2 (2019)		✓														✓						onoM2M and OCF
oneM2M TS-0026-V3.3.0 (2019)		✓														✓						oneM2M and 3GPP
oneM2M TS-0030-V3.0.2 (2019)		✓							✓							✓						

Note that abbreviations in the related security factors column denote the following:
data protection (DP), framework (FR), general (GE), network (NET), privacy (PR), protocol (PT), secure access (SA), and usecase (UC)

number of elements (i.e., interface definition, network description, security capabilities, security parameters, and entity metadata including data type, capabilities description, and constraints). ISO/IEC 21823-1:2019 also introduces a framework for interoperable IoT systems based on an IoT reference architecture standard (i.e., ISO/IEC 30141:2018 [96]). Fig. 4 shows a simplified version of the IoT reference architecture included in ISO/IEC 21823-1. Specifically, the interaction

TABLE III
OVERVIEW OF SECURITY-RELATED INTERNATIONAL STANDARDS FOR IoT

Standard Name	Security related factors										Limitation					Interoperability related factors	Domain
	General	Usecase	Network	Framework	Architecture	Protocol	Secure access	Data protection	Privacy	Policy	Platform specificed	Conceptual	Low accessibility	Market gap	Lack of developer support		
IEEE 1609.0 (WAVE) (2019)	✓							✓					✓		✓	AR	WAVE
IEEE 1609.11 (2010)							✓						✓		✓	TP_Dist_PT	WAVE
IEEE 1609.2 (2016)			✓			✓	✓	✓					✓		✓		WAVE
IEEE 802.11 (Wi-FI) (2016)			✓			✓	✓	✓		✓			✓		✓	TP_Dist_PT	Wi-FI
IEEE 802.15.4 (WPAN) (2011)								✓					✓		✓	TP_Dist_PT	WPAN
IETF RFC 7925 (2016)	✓					✓						✓			✓	TP_Dist_PT	CoAP
IETF RFC 8323 (2018)	✓					✓									✓	TP_Dist_PT	CoAP
ISO/IEC 20248:2018 (2018)						✓	✓		✓				✓		✓	DEF	RFID
ISO/IEC 20922:2016 (MQTT) (2016)	✓					✓	✓		✓					✓		BE, SEM, SYN, TP_Dist_PT	MQTT
ISO/IEC TR22417:2017 (2017)	✓	✓	✓						✓			✓	✓		✓	UC	
ITU-T X.675 (2015)	✓														✓	FR, ID	Object identifies
ITU-T Y.2060 (2012)	✓											✓			✓	RM	
ITU-T Y.2063 (2012)	✓											✓			✓	AR, FR, REQ	WoT
ITU-T Y.2066 (2014)	✓											✓			✓	REQ, UC	Common IoT
ITU-T Y.4101/Y2067 (2017)	✓											✓			✓		Gateway of IoT
ITU-T Y.4111/Y2076 (2016)	✓											✓			✓	FR, REQ, RM, SEM	
ITU-T Y.4112/Y2077 (2016)	✓											✓			✓	REQ	PnP
ITU-T Y.4553 (2016)	✓											✓			✓	REQ	SPSN
ITU-T Y.4702 (2016)	✓											✓			✓	REQ	Device management
OCF Core Specifiation (30118-1:2018) (2019)				✓							✓					AR, DEF, RF, SEM, TP_Dist_GE, TP_Dist_PB	
OCF Security Specification (OCF-Sec) (2019)	✓		✓	✓		✓	✓	✓	✓		✓						
oneM2M TR-0001-V3.1.1 (2019)	✓										✓					REQ, UC	
oneM2M TR-0010-V3.0.1 (2019)	✓										✓					TP_Dist_PB	oneM2M and MQTT
oneM2M TR-0018-V2.5.1 (2019)	✓										✓					REQ, UC	
oneM2M TS-0003-V3.11.0 (2019)	✓			✓	✓	✓	✓	✓	✓	✓	✓						oneM2M
oneM2M TS-0004-V3.15.0 (2020)	✓										✓					TP_Dist_PB, TP_Dist_PT	
oneM2M TS-0009-V3.5.0 (2019)	✓										✓					TP_Dist_PB	oneM2M and HTTP
oneM2M TS-0020-V3.0.1 (2019)	✓										✓					TP_Dist_PB	oneM2M and WebSocket

Note that abbreviations in the related security factors column denote the following:
architecture (AR), behavioural (BE), definition (DEF), framework (FR), identifier (ID), requirement (REQ), reference model (RM), semantic (SEM), syntatic (SYN), transport general (TP_Dist_GE), transport protocol binding (TP_Dist_PB), transport protocol (TP_Dist_PT), and usecase (UC)

among entities and different systems in an IoT system are shown. In addition, the standard briefly mentioned security for interoperability in terms of the following three factors: confidentiality, integrity, and protection of personal identifiable information. The standard indicated that these three security factors should be guaranteed between two interoperating IoT systems for interoperability, and the protection of personal information may impact behavioral and policy facets.

ISO/IEC 20924:2018 [1] is titled "Information technology-Internet of Things (IoT)-vocabulary" and it describes a definition of IoT along with a set of terms and definitions. The purpose of this standard is to form a terminology foundation for IoT; thus, the standard defines a variety of IoT terms in detail based on other standards or its own definition. This standard does not solve technical interoperability problems but can help with terminology interoperability between IoT documents. This standard only considers the interoperability of terminologies for IoT; thus, security factors are not taken into account.

ISO/IEC TR 22417:2017 [97] is a technical report and titled "information technology-Internet of Things (IoT) use cases" This technical report identifies several of the 25 IoT scenarios and 14 use cases that are based on real-world requirements

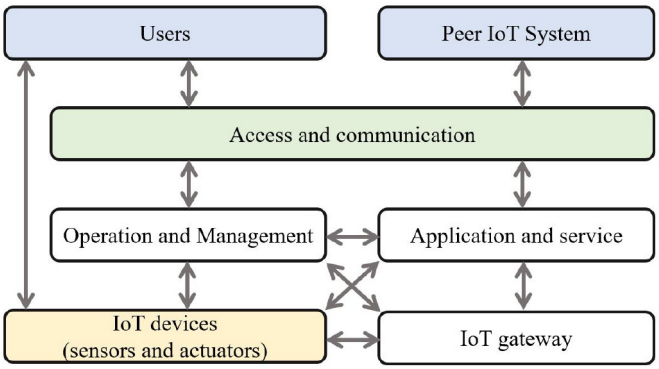

Fig. 4. Interaction among entities in IoT System from ISO/IEC 21823-1:2019 (re-drawed).

and applications. The purpose of the technical report is to provide a practical context for considerations of interoperability based on user experience. Therefore, scenarios and use cases can be applied in IoT research or standardization as a unified example. In addition, some scenarios (i.e., integrated smart pump system, IoT endpoint monitoring system, and IoT-based energy management system for industrial facilities) directly refer to interoperability problems in information exchange, and these interoperability problems must be solved before accomplishing the objectives of each scenario. In addition, two scenarios are related to security: IoT network security and IoT security threat detection and management. The former scenario describes that telecommunications companies offer telecommunication services to IoT providers for various services with rapid provisioning of IoT services (i.e., new agile security capabilities and functionality enabling IoT security). The latter scenario is related to security in the cloud services used by the IoT. In this scenario, telecommunication cloud service providers can gather a large amount of IoT data (e.g., endpoint, status, and utilization) and analyze the collected data. The gathered data can then be used for centralized threated detection and mitigation via intelligent security policy enforcement. Furthermore, all of these scenarios in ISO/IEC TR 22417:2017 consist of 12 detailed subsections: scope and objectives of use cases, narrative of use cases, actors, problems (legal constraints, legal regulations, and constraints), referenced standards and/or standardization committees, relation with other known use cases, general remarks, security and privacy, conformity aspects and critical requirements, interaction between actors and user requirements, drawing or diagram of use case, and data flow diagram of use case. Therefore, security-related factors can be found in the security and privacy subsections.

ISO/IEC 20922:2016 [98] is based on a de facto standard by OASIS, which is a global nonprofit consortium for open standards, including the IoT. The standard name is "information technology - message queuing telemetry transport (MQTT) v 3.1.1" which contains a client-server publish/subscribe messaging transport protocol in TCP/IP, and the protocol is lightweight, open, and designed to be implemented easily. The characteristics of MQTT are useful for IoT or machine-to-machine (M2M), and the protocol can be a solution for the interoperability of message exchange between IoT devices (i.e., MQTT provides a syntactic format for data exchange). In addition, MQTT also includes semantic rules for labeling, but the rules only provide regulations for MQTT packets. MQTT also provides security guidance, but is non-normative. However, the National Institute of Standards and Technology (NIST) and OASIS provide MQTT and the NIST cyber cybersecurity frameworks [99] with a way of improving critical infrastructure cybersecurity for MQTT consistent with the NIST framework. However, ISO/IEC 20922:2016 is based on the previous version of MQTT (i.e., v3.1.1), but the newest version has been published in OASIS (i.e., 5.0 [100]).

Radio frequency identification (RFID) is operated in close proximity of up to 10 m, and this network protocol can be applied in an IoT network [101]. The ISO/IEC 18000 series [102]–[111] describes diverse RFID protocols via several frequency ranges. In addition, ISO/IEC 20248 describes public-key infrastructure digital signatures and certificate technologies and specifies a digital signature data structure for RFID authentication.

ISO/IEC 30118-1:2018 [112] focused on the Open Connectivity Foundation (OCF) specification. OCF is an industry organization for developing IoT-related de facto standards, interoperability guidelines, and providing a program for devices [76]. However, ISO/IEC 30118-1:2018 describes the core specifications of the OCF framework, architecture, interface, and resource model for interoperability in IoT. Details of the OCF standards are described in Section VI-F.

In summary, ISO/IEC JTC 1 considers different perspectives for interoperability and security in the IoT, such as definition, conceptual informatics, and network protocols.

B. IEEE-SA Standards

IEEE-SA has several network-related standards. IEEE 802 is a family of IEEE standards for LAN and MAN, and the standard family contains several wired and wireless network protocols (e.g., WPANs [65]–[69], [113]–[116] and WiMax WiMax [117]–[119]). However, wired network technologies are used in an IoT environment in the background, and network protocols observe many related standards. It is beyond the scope of this paper to analyze every network-related standard; thus, we only focused on core IEEE network standards for wireless networks for IoT. Therefore, we analyzed IEEE 802.11 [38] (i.e., Wi-Fi) and IEEE 802.15.4 to 5 [65]–[69], [115] (i.e., Bluetooth, ZigBee, WirelessHART, 6LoWPAN, Thread®, and Z-Wave). However, network protocols can solve transport interoperability because these standards can help with the exchange of data between IoT entities. Therefore, we classified the network protocol standards as transport interoperability in Table II.

Wi-Fi is a wireless network protocol for local area networks (i.e., short to medium range up to 1000 m [101]), and Wi-Fi follows the IEEE 802.11 ecosystem. The protocol is maintained by the working group WLAN standards in IEEE-SA [120] and Wi-Fi Alliance [121]. Wi-Fi is designed with high-bandwidth data (e.g., video streaming and file sharing), and it can be operated by user-owned devices. Therefore, the

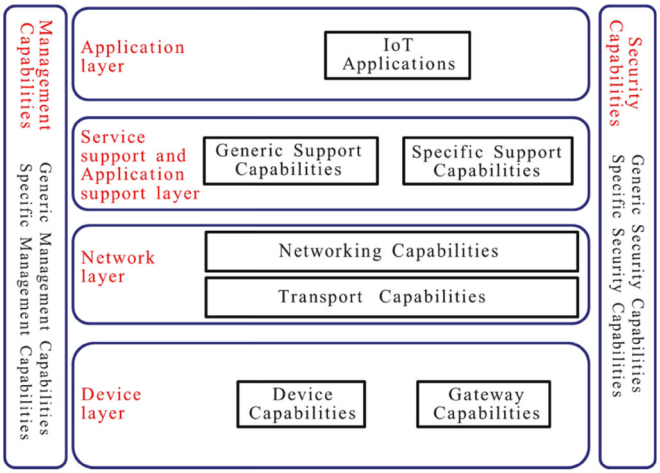

Fig. 5. IoT reference model (ITU-T .4000/Y.2060) [128].

protocol can be widely used in an IoT environment [101]. In addition, IEEE 802.11 includes security concerns, and they classified two definitions for security algorithms based on robust security network associations (RSNA): RSNA algorithms and pre-RSNA algorithms. RSNA is a logical connection between entities using IEEE 802.11 via IEEE 802.11.i key management scheme [102] (i.e., four-way handshake). Details of security algorithms and methods are out of the scope of this paper, but IEEE 802.11 includes authentication, authorization, access control, encryption, key cryptography, data confidentiality, data authenticity, reply protection, and policies for Wi-Fi protocols.

Wireless personal area networks (WPAN) provide a short-range network area of up to 100 m. Bluetooth, ZigBee, WirelessHART, 6loWPAN, and Z-Wave are several WPAN protocols that can be used in IoT environments with different characteristics, but the protocols are based on IEEE 802.15.4 and IEEE 802.15.5 [65]–[69], [101], [115]. IEEE 802.15.4 describes a protocol and compatible interconnection for data communication devices [65], and the devices used low data rates, low power, and low complexity in WPAN. IEEE 802.15.4 provides transport interoperability, and it denotes specific security services: data confidentiality, data authenticity, and replay protection [65]. IEEE 802.15.5 is based on IEEE 802.15.4 and supported for security services, but this standard was developed for a mesh network.

IEEE 1609 series [122]–[126] designated for wireless access in vehicular environments (WAVE), and the series are related to IEEE 802.11 [127]. The series classified its standards by functionality and usability (i.e., architecture, protocol, security, and identifies). IEEE 1609.0 [122] provides guidance for architecture and services to communicate between WAVE devices in a mobile vehicular environment. In addition, this standard describes generic security considerations for WAVE. IEEE 1609.3 [124] specifies networking services for WAVE devices and systems, and it provides protocols for WAVE short message services. In addition, IEEE 1609.11 provides protocols for over-the-air electronic payment data exchanged in intelligent transportation systems [125]. IEEE 1609.2 [123] defines secure message formats and processing WAVE devices. IEEE 1609.12 [126] is presented for the identification and use of the identifiers for WAVE.

In summary, IEEE-SA developed various network protocols to solve transport interoperability, and the standards considered security-related factors in networking.

C. ITU-T Standards

ITU-T classified their standards (i.e., recommendations) as series A to Z through several topics. In particular, series Y is a set of global information infrastructure, Internet protocol aspects, and next-generation networks, and the series has IoT-related recommendations. In addition, series F (non-telephone telecommunication service) and series X (data networks, open system communications, and security) are also related to IoT recommendations. Details of IoT related to each series are described below.

ITU-T Y.4000/Y.2060 is a recommendation for an overview of IoT [128], and this recommendation is referenced by other IoT-related recommendations in ITU-T. This recommendation provides a concept, scope, characteristics, high-level requirements, and a reference model for IoT. In addition, the ecosystem and business models are provided as informative appendices. The recommendation also emphasizes interoperability and security as high-level requirements of the IoT. We supposed that the IoT reference model provided by ITU-T Y.4000/Y.2060 can be a solution for interoperability problems. As shown in Fig. 5, the IoT reference model consists of four layers: application, service support and application support layer, network layer, and device layer. The application layer contains IoT applications. The service support and application support layers are divided into generic or specific support capabilities. The generic support capabilities can be used by different IoT applications for conventional capabilities (e.g., data processing or data storage). Specific support capabilities support particular capabilities for diversified IoT applications. The network layer consisted of two types of capabilities. The network capabilities provide control functions to guarantee network connectivity. Transport capabilities are responsible for providing connectivity among IoT services and application-specific data information. In the device layer, device and gateway capabilities exist. The device capabilities include direct and indirect interactions with the communication network, ad-hoc networking, and sleeping and waking up. The gateway capabilities include multiple interface supports and protocol conversion. However, the device layer capabilities are not limited, as described. Security and management capabilities affect four layers. The security capabilities consisted of generic and specific capabilities. The generic security capabilities affect the application, network, and device layers, and the specific security capabilities are related to application-specific requirements. Management capabilities can also be classified as generic and specific. The generic management capabilities are responsible for devices, local network topology, traffic, and congestion management. Specific management is closely related to specific requirements from IoT applications. In addition, the standard includes the relationships between different

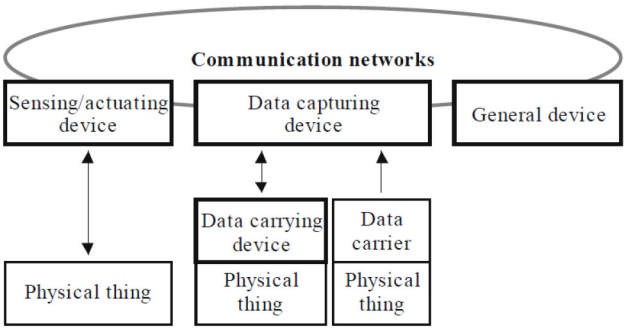

Fig. 6. Relationship between different types of devices with physical entities (ITU-T Y.4000/Y.2060) [128].

types, devices, and physical entities. There are physical and virtual entities. Virtual entities can exist without physical entities. However, devices communicate with each other through a communication network. Data-capture devices (i.e., data carrying devices, data carriers, and data capturing devices) are required to interact with physical entities in some cases. Fig. 6 shows the types of devices and their relationship. It should be noted that general devices are sets of physical entities.

ITU-T Y.4400/Y.2063 [129] includes a framework of the Web of Things (WoT), which is a special type of IoT. Unlike the IoT, WoT is defined as "a way to realize IoT where (physical and virtual) things are connected and controlled through the World Wide Web" [129]. The recommendation specifies requirements for WoT, and the requirements are classified into general and functional aspects. The general requirements can be summarized as requiring physical devices, providing access to Web resources for physical devices, interoperability among different networks and operating systems, and supporting compatibility between different data formats. The function requirement for WoT reflects the supporting functional aspects, such as service profile management, service control, service composition, access control, physical device access via the Web, agent resource management, and mapping information between devices and agents. In addition, ITU-T Y.2063 provides WoT architecture, and its architecture consists of three layers: service, adaption, and physical. Fig. 7 shows an overview of the WoT architecture. The service layer provides a common function for service capabilities and is responsible for making and managing the services. The adaptation layer is responsible for resource and agent management. The agents are located in the adaptation layer, and the agents interact with physical devices for translation from different protocols and messages. Dependent on the device type, the correspondence agents in the adaptation layer are connected. Physical devices are in physical layers, and all devices can be accessed by the agents in the adaptation layer. In addition, the recommendation provides general security considerations for WoT.

Several recommendations provide common requirements from a different perspective. Providing requirements can help to develop IoT applications and systems with an interoperability view; thus, we included requirement related standards. ITU-T Y.4100/Y.2066 provides common requirements of IoT based on ITU-T Y.4000/Y.2060, and the requirements are provided in detail based on general use cases and actors in IoT. However, ITU-T Y.2068 [130] describes the capabilities of the IoT needed to fulfill the requirements specified in ITU-T Y.2066. ITU-T Y.4101/Y2067 [131] includes common requirements of a gateway for IoT applications with generally applicable scenarios (i.e., a gateway in home service, automotive telematics, and online collaborative whiteboard). ITU-T Y.4702 [132] provides a common requirement and capabilities for device management for IoT. ITU-T Y.4553 [133] has the requirements of a smartphone as a sink node (SPSN) for IoT applications and services. A sink node in IoT is defined as "collects and/or transfers information for/to a group of IoT devices at an end-user network" SPAN means that a smartphone can support functionalities as a sink node. The recommendation contains descriptions and characteristics of SPSN and its requirements for several use cases (i.e., commercial merchant services, home services, environment-monitoring services, and wearable smart devices). Plug and play (PnP) is the concept of capability for satisfying requirements when devices are connected, and autonomic generation and acquisition of the configuration are needed to accomplish PnP [134]. ITU-T Y.4112/Y2077 [134] provides the requirements of PnP capability for IoT. ITU-T Y.4111/Y.2076 includes semantics-based requirements and a framework for IoT. In this recommendation, the term semantics is used as "the rules and conventions governing the interpretation and assignment of meaning to construction in a language" In addition, the recommendation classified four layers and defined the relationship between the layers to represent a semantic-based capability framework. The layers consist of an application layer (AL), a network layer (NL), a device layer (DL), and service support and an application support (SSAS) layer. Each layer is related to semantic security support capabilities (SSSC) and semantic management support capabilities (SMSC). Fig. 8 shows the semantic capabilities in an IoT reference model [135]. The directional arrows in the figure indicate that a directing layer can be invoked by a directed layer or capabilities. All requirement recommendations [131]–[135] commonly contain general security requirements.

ITU-T X.675 [136] provides an object identifiers (OID) - based resolution framework for heterogeneous identifiers and locators. Identifying various resources can provide interoperability among heterogeneous identifiers in the IoT. The recommendation includes an OID-based resolution for the framework and requirements for identifiers and locators. The framework is explained with a simple example and its registration processes, and two scenarios, depending on the presence or absence of a gateway. In addition, the requirements consist of eight topics, as follows.

- Support of independence from existing identifiers' operation
- Support of both identifiers and locators
- Support of heterogeneous existing identifiers
- Guarantee uniqueness of existing identifiers
- Support of new identifiers
- Support for fault tolerance and stability

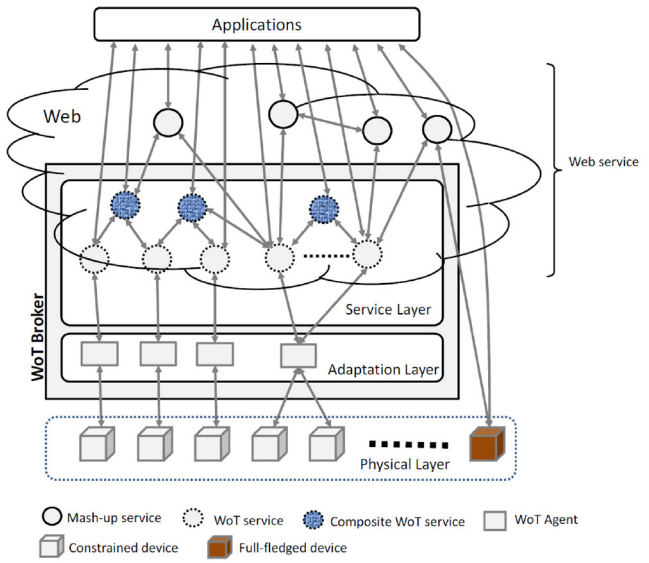

Fig. 7. Overview of WoT architecture (ITU-T Y.4400/Y.2063) [129].

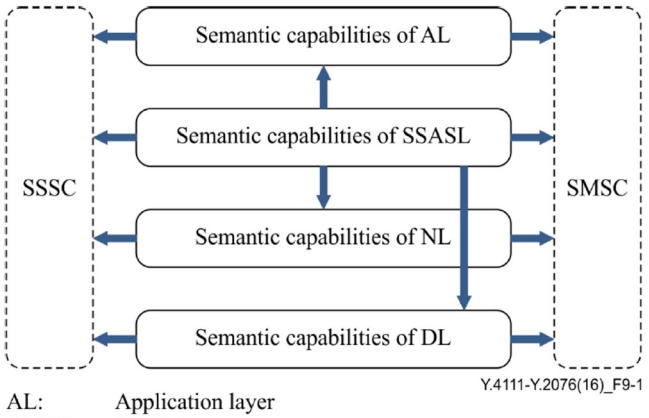

Fig. 8. Semantic capabilities in the IoT reference model (ITU-T Y.4111/Y.2076) [135].

- Support for end-to-end identification
- Support for authentication and authorization

In summary, the recommendations of ITU-T provide an overview, frameworks, architecture models, requirements, and capabilities for various IoT perspectives for interoperability, and the recommendations consider security factors to protect data and privacy.

D. IETF Standards

IETF has several RFC series (i.e., proposed standards and informational specification), but there is no STD series (i.e., Internet standard) for interoperability and security in IoT. However, some RFC specifications can be translated as STD series if its maturity is high enough (i.e., RCF series for standard track) [90]. First, we analyzed the RCF series on a standard track. RFC 8323 [137] provides the constrained application protocol (CoAP), which was designed for IoT [39] over TCP, TLS, and WebSocket [40]. CoAP is developed for constrained devices (i.e., nodes); thus, the devices can communicate over the wider Internet vie CoAP. In addition, CoAP can also be applied to networks among devices in constrained networks such as low-power and lossy networks. The characteristics of CoAP have been appropriated to apply to an IoT network; thus, CoAP may solve transport interoperability. In addition, RFC 8323 includes security considerations applied from previous RFC specifications (i.e., CoAP [39] and WebSocket [40]). The considerations are described below.

- Parsing protocol and processing URIs
- Proxying and caching
- Risk of amplification
- IP address spoofing attacks
- Cross-protocol attack
- Constrained node consideration
- Non-browser clients
- Origin considerations
- Attacks on infrastructure (masking)
- Implementation-specific limits
- WebSocket client authorization
- Connection confidentiality and integrity.
- Handling of invalid data
- Use of SHA-1 by WebSocket handshakes

RFC 7925 [138] includes Internet security protocols to protect messages (i.e., CoAP), which use transport layer security (TLS) [139] and datagram transport layer security [140]. RFC 7925 is focused on the IoT environment with constrained devices that collect data via sensors or control actuators (e.g., home automation, industrial control systems, and smart cities). RFC 7925 is mainly focused on the security of the CoAP protocol [39] using TLS 1.2 [139] and DTLS 1.2 [140]. The TLS protocol provides authenticated, confidential, and integrity-protected communication between two endpoints, and DTLS is similar to TLS but operates on top of an unreliable datagram transport. Therefore, the specification considers security considerations, such as credential types, signature algorithms, error handling, session hash, renegotiation attacks, downgrading attacks, crypto agility, and privacy considerations.

Moreover, there are informational RFC series in IETF that are not a standard, but there is referenceable information for research and standardization of interoperability and security in IoT. For example, RFC 8576 [141] includes state of the art of and challenges for IoT security, and the specification is produced in IRTF T2TRG. RFC 8352 also includes challenges for energy-efficient features of IoT protocol operation on constrained devices and current practices to overcome the challenges [142]. RFC 8352 is also an informational specification that [142] only considers an energy-efficient feature protocol but not security. In addition, the IETF provides specifications the workshop report for IoT interoperability problems. RFC 8477 [143] provides a summary of the workshop on IoT semantic interoperability, and the report contains problem solving for interoperability such as formal languages, debugging support, translation, and runtime discovery. In addition, the report indicates security considerations for semantic

interoperability. The considerations are the use of formal data models and security of data and data models in general.

E. oneM2M Standards

Recently, oneM2M released the fifth version for standards and technical reports; however, we analyzed only the third release. The fourth and fifth releases are provided for information only, and the releases need to be improved before formal publication, as described in Section V-E. In addition, most of the standards and technical reports published by oneM2M consider M2M technology; however, M2M technology is one of the fundamental technologies for IoT; thus, we also analyzed M2M standards.

Security-related applicable solutions within the oneM2M based system are presented in TS-0003-V3.11.0 [144]. The standard describes security-related considerations in great detail, including security architecture, security services and interaction, authorization, security framework, security framework procedures and parameters, protocols and algorithms, privacy protection architecture, and security-specific oneM2M data type definition. However, TS-0016-V3.0.2 [145] describes an abstraction of the secure environment (SE) that is defined in TS-0003-V3.11.0 [144] in more detail. SE is defined as as a "logical entity that protects sensitive data, and sensitive functions from tampering, unauthorized monitoring or execution and that provide access to these sensitive data and sensitive functions to authorized oneM2M entities" [144]. In particular, the abstraction standard focused on the specification of mechanisms and interfaces of abstracts in a secure environment from diriment technical implementation. However, interoperability is not considered in security-related standards.

oneM2M developed protocol-related specifications to solve transport interoperability [146]–[150]. TS-0004-V3.15.0 [146] provides a specification of the communication protocols for a oneM2M based system, including common data formats, interfaces, and message sequences. In addition, security factors were considered in the protocol. Further, oneM2M provides binding specifications to support other protocols. TS-0006-V3.6.2 includes specifications between the oneM2M protocol and the Customer-premises equipment WAN Management Protocol (CWMP) [151], which was developed by the broadband forum [93]. TS-0008-V.3.5.0 [147] provides binding specifications with CoAP, which is a protocol defined by IETF [39], and the binding standard includes security considerations for the binding. TS-0009-V3.5.0 [148] provides a protocol with binding specifications between the oneM2M protocol and hypertext transfer protocol (HTTP), and security-related considerations are included. MQTT [98] is the ISO/IEC JTC 1 standard for IoT protocols developed by OASIS, and TR-0010-V3.0.1 [149] provides binding MQTT and oneM2M protocols. The binding with MQTT provides security considerations, and especially, authorization and authentication are emphasized. TS-0020-V3.0.1 [150] includes binding with WebSocket [40], which is a protocol for IoT developed by IETF.

To support semantic interoperability, oneM2M developed standards and technical reports. TS-0012-V3.7.3 [152] provides ontology-based OWL for oneM2M, and this standard also specifies the instantiation of the ontology for oneM2M resources that can be used for semantic annotation and interworking. In addition, mapping with the Smart Appliances REFerence (SAREF) ontology [152] developed by ETSI is provided. The ontology is used to specify semantic functions for oneM2M in TS-0034-V3.0.2 [153]. TS-0023-V3.7.3 [154] provides definitions of information models for home appliances based on oneM2M and mapping with other information models based on other platforms. TR-0033-V3.0.0 [155] provides requirements for semantic enablement and approaches for addressing the requirements.

Interworking among oneM2M and other platforms is being developed. TS-0024-V3.2.2 [156] provides interworking between oneM2M specified entities and the OCF-specified client/server. TS-0026-V3.3.0 [157] contains interworking with a 3rd generation partnership project (3GPP) [158]. In particular, the standard focused on the service layer of oneM2M in the 3GPP network; thus, IoT-related 3GPP features are used for the oneM2M service layer. In addition, a technical report [159] for developing interworking between oneM2M and 3GPP was published with a use case (i.e., a water meter application). TS-0030-V3.0.2 [160] describes generic interworking using ontology [161] to interwork between oneM2M systems and external systems. TS-0035-V3.0.0 [162] provides principles and guidelines for interworking between oneM2M systems with the Open Service Gateway initiative (OSGi) [163] framework. The interworking also includes interworking devices and gateways based on OSGi. TS-0033-V3.0.0 [155] introduces a framework including interworking methodologies between oneM2M and external proximal IoT technologies. The proximal IoT is defined as "IoT components communicating with each other directly in a local network using specific communication protocols and information models [155]" However, not all interworking standards are considered security-related considerations in interworking processes.

Several technical reports provide use cases and requirements for different M2M domains [146], [164], [165]. TR-0001-V3.1.1 [164] includes a collection of use cases that focus on the interaction between actors and potential requirements for various industry segments. The industrial use cases consist of energy, enterprise, healthcare, public services, residential, retail, transportation, and others. In addition, each use case includes a description, source, actors, pre-condition, triggers, flow of a sequence of interactions between actors and the system, illustrations, and potential requirements. In potential requirements, most of the use cases include security-related requirements. TR-0018-V2.5.1 [165] also collected use cases (i.e., on-demand data collection for factories, integrity of data collection monitoring, data processes for inter-factory manufacturing, aircraft construction and maintenance, real-time data collection, data encryption, QoS monitoring, and QoI monitoring) and requirements (i.e., high-level architecture

and security analysis) of the industrial domain. In particular, TR-0018-V2.5.1 considers security-related analysis, including identification, authentication, use control, data confidentiality, system integrity, and restricted data flow. TR-0026-V3.0.1 [157] describes use cases and requirements for the vehicular domain, and 18 very specific use cases are described. There is a security-related use case (i.e., vehicle location privacy protection), and many use cases are considered as security-related factors. In addition, potential requirements and potential solutions are introduced, and security is one of the problems.

In summary, standards and technical reports from oneM2M detail specifics of their system in various research fields (e.g., protocol, architecture, requirement, interworking, and use cases); however, the standards and technical reports provide specifications that can be applied to their system. Therefore, generic interoperability and security problems are rarely considered.

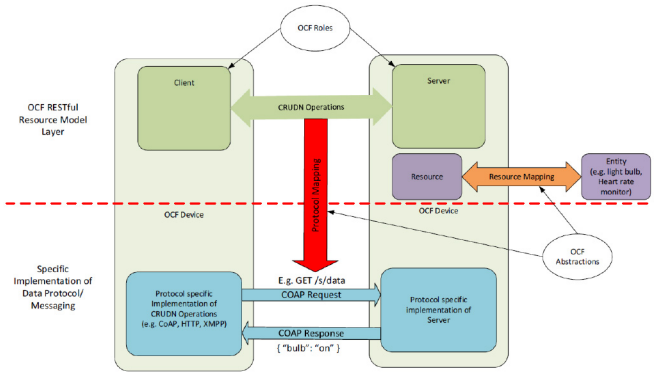

Fig. 9. Architecture of IoT (OCF core specification) [167].

F. OCF Standards

The OCF released the lasted internal standards on February 2020 (i.e., OCF specification 2.1.1), which consisted of 16 different topics [166]. OCF also provides a draft version of specifications to improve existing specifications, but the drafts are not considered in this paper. As described in Section V-A, ISO/IEC 30118-1:2018 [112] is based on the OCF specification. Note that OCF standards have no specific document number; thus, we used abbreviations of each OCF standard to enhance readability. OCF core specifications (OCF-CS) [167] cover the overall OCF framework; thus, OCF-CS is mandatory for all devices that use the OCF framework. The standard describes core architecture, interfaces, protocols, resource model, network, and services for OCF-based implementations in IoT environments; therefore, the standards include several interoperability factors. Fig. 9 shows an overview of the OCF architecture, which consists of a resource model, representational state transfer (RESTful) operations, and abstractions. The abstractions are used in the resource model and RESTful operations to map concrete elements using abstraction primitives. The resource model provides abstractions and concepts for logical models, and it logically operates on applications and environments. The architecture operations are based on RESTful, an architecture defined as a set of constraints for Web services. The operations are defined using generic CRUDN operations, namely, CREATE, RETRIEVE, UPDATE, DELETE, and NOTIFY. CoAP is used as a messaging protocol; thus, CRUDN operations are mapped to CoAP. The details of the OCF architecture are described in OCF-CS. Moreover, several standards published in OCF have been developed to supplement OCF-CS.

OCF Core Optional Specification (OCF-COS) [168] describes optional specifications that can be implemented on any device using the OCF framework. In particular, OCF-COS specifies functional interactions and resource type definitions.

Based on OCF-CS, OCF provides device-related standards. OCF Device Specification (OCF-DS) [169] specifies very detailed device definitions based on the OCF-CS. The OCF Device to Cloud Service Specification (OCF-DCSS) [170] includes extended device definitions to apply OCF-CS to the cloud environment. The OCF also provides a bridging framework (OCF-BS) [171] for translation between OCF devices and other IoT ecosystems. The bridging framework provides general requirements, device types, and resource types to generate a bridge between OCF devices and others.

In addition, there are resource-related standards to define resources in detail. OCF Resource Type Specification (OCF-RTS) [172] specifies detailed definitions of resources used in OCF-CS, and the resource definitions include model construction and resource-type definitions. The OCF Wi-Fi Easy Setup Specification (OCF-WFESS) [173] defines new resource types that apply to Wi-Fi easy setups, including resource model, network and connectivity, and functional interaction. Several standards [62]–[64], [174]–[176] are defined by mapping between the defined resource in OCF and various IoT protocols and platforms (i.e., Z-Wave [63], ZigBee [64], UPlus [174], oneM2M [175], Bluetooth Low Energy (BLE) [62], and AllJoyn [176]). However, OCS-CS-based standards for the device and resource may help solve interoperability problems, but Table II only reflects OCF-CS because the other optional standards are included in OCF-CS only in an overall view.

OCF-CS denotes that security and privacy are specified in the OCF Security Specification (OCF-Sec) [127], and OCF-Sec is also defined in ISO/IEC 30118-2:2018 [177]. The OCF-CS specifies the security objectives, philosophy, resources, and mechanisms of an OCF environment. More specifically, OCF-Sec includes provisioning, credential-related management, message integrity and confidentiality, access control, security resources, and guidelines for security. OCF Cloud Security Specification (OCF-SecC) [178] defines security-related informative contents for OCF in a cloud environment.

In short, OCF provides its IoT framework in detail with interoperability and security. However, they focused on interoperability and security for their framework, not for general purposes.

VII. Discussion, Open Challenges, and Future Direction

Herein, we discuss open problems and challenges related to standardization in relation to interoperability and security in IoT environments. We also discuss future research directions.

A. Rapid Process for Standardization (Market Gap)

As described, several de jure standards follow de facto standards such as ISO/IEC 20922:2016 (MQTT) and ISO/IEC 30118-1:2018 (OCF framework). However, the publication cycle for de facto standards is rapid compared with that for de jure standards; for example, MQTT is published in a new version (5.0) in April 2019, but ISO/IEC 20922:2016 is based on the old version of MQTT published in November 2014. Because de jure standards have to include several factors, including agreement between standard members and agreement of chair committees, standard cycles are slower than de facto publication cycles. It is important to consider details when publishing international standards, but a fast standardization cycle may reflect market needs more efficiently and in a timely manner. Therefore, a faster standardization cycle and open access before publication are considered part of the de jure standardization process.

B. Standards Considering Interoperability and Security

De facto standardization organizations, such as OCF and oneM2M, have their own platforms and standards for utilizing their platforms. Further, standards are provided on interworking between the platforms and other IoT-related standards such as protocols, case studies, and other platforms. Interworking helps manufacturers and users to apply or interwork with their platforms. However, in the interworking process, security must be considered to prevent security-related problems; for example, an interoperable access control framework can be applied for secure-access between different IoT platforms [179], [180]. In addition, an identification method may be applied for interoperability among devices from different platforms [181], [182].

C. Interoperability for Network Protocol

There are several network protocol standards that are applied in IoT (e.g., Bluetooth, RFID, Wi-Fi, MQTT, WebSocket, and ZigBee), and an interoperable protocol interface is needed among different protocols. In an IoT environment, devices can communicate directly with each other, and a smooth interconnection is needed for interoperable communication. However, efficiency must be considered when developing an interoperable interface between IoT devices because some IoT devices need to be operated with low battery consumption and low computing power. Further, these specifications can be responsible for security threats (e.g., exhaustion, unfairness, hello flood, flooding, side-channel attack, overwhelm, and denial of sleep) [30], [101].

D. Automated IoT Systems

To support fully automated IoT environments, IoT systems and devices must have the possibility of connecting, disconnecting, transferring data, making decisions, and actuating automatically. In other words, there is a requirement for minimizing human intervention as much as possible during the operation of IoT systems. From this perspective, the concept of self-adaptive software may be applied to IoT. Self-adaptive software can be defined as a software that detects environmental conditions and changes its behavior or structure if the requirements are violated [183], and it has been applied in several IoT research studies on modeling [184], verification [185], [186], and authentication [187]. However, to apply self-adaptivity to IoT environments, semantic interoperability must be considered. Further, security-related topics in IoT can also be applied to the concept of self-adaptive software such as dynamic access control, authorization, and authentication. In addition, blockchains have recently attracted attention in IoT research, and several studies have been conducted on applying blockchains in IoT [188]–[190]. The characteristics of blockchains, such as decentralization and openness, may help to implement secure IoT environments; thus, an optimization between IoT and blockchains is important for IoT.

E. Standardization for Semantic Interoperability

Matching data and services is a demanding task. Moreover, it is difficult to develop automatic matching methods [55], [70]. Several IoT service providers use their own definitions of resources and services. It is difficult to unify definitions and service ranges among different IoT services. In addition, several IoT platforms have their own data description and resource expressions, and this can cause difficulties in developing IoT environments. Therefore, to address these issues, reasonable semantic concepts and methods, including reasoning, are required for interoperability in IoT. Several studies [32], [49], [55] have focused on semantic interoperability. This can be a solution in specific domains (e.g., INTER-IoT and WoT). However, there are several working groups that address semantic interoperability. For example, ISO/IEC JCT 1 SC 32 focused on data management and interchange, and provided standards to promote harmonization of data management (e.g., definitions of data domains, data types, data structures, associated semantics, and data interchange). In addition, IEEE-SA provides interoperability in several areas, such as smart grids, software reuse, and clouds. However, to address semantic interoperability in general for IoT, general definitions of IoT resources and services are required for the development of IoT environments. Therefore, standardization can be a general solution for semantic interoperability so that IoT services and environments can be developed.

F. Low Accessibility and Lack of Developer Support

Currently, international standards can be downloaded through the official website and libraries of an organization [71]–[76]. In addition, de facto standards can be downloaded free of charge, and some de jure standards based on de

facto or open standards (e.g., ISO/IEC 20922:2016 [98] based on MQTT [100]) can be acquired free of charge. Nevertheless, although some standards (e.g., ISO/IEC 30118-1:2018 [112]) are based on an open standard (OCF Core Specification [167]), which is free, a payment is required to obtain them. This payment policy in standards organizations can act as a barrier to researchers and developers, and can cause low accessibility. In addition, low accessibility can also be caused by inadequate support for IoT developers. Several de facto standards based on specific frameworks, platforms, or protocols (e.g., oneM2M platform, IoTivity framework, and MQTT protocol) provide material to aid IoT developers, such as guide documents, wiki, tools, and open source projects, on their official Web site [94], [191]–[197]. Nevertheless, several standards provide only documents without support for IoT developers, and thus they are difficult to apply in the development process. In this case, several open-source projects or APIs have been used to apply the standards. However, security cannot be ensured if open-source projects and APIs are used, and in fact, severe security problems may be caused. Therefore, it is necessary that supporting material (such as official source code, APIs, technical reports, technical specifications, and guidelines) be provided to developers so that security and proper usage may be ensured.

G. Conceptual Content

Several standards provide conceptual content for interoperability and security in an IoT environment, such as architecture, framework, and requirements. Conceptual standards are important for establishing a general-purpose IoT system and environment. However, in some cases, researchers and IoT developers make empirical assumptions to address interoperability and security problems through the standards. Therefore, standards organizations should publish technical reports containing specifications and guidelines to provide practical content that can enhance the level of interoperability and security in IoT environments. In addition, research is required to specify the conceptual content using IoT examples.

H. Platform Specified Standards

Several standards developed by de facto standards organizations (i.e., open standards organizations) are based on specific platforms and frameworks; for example, oneM2M standards are developed to support the oneM2M platform, and OCF standards are developed to support the IoTivity framework. In addition, organizations provide standards to interwork with other standards or technologies (e.g., protocol binding and ontology mapping). However, platform providers define several rules to interwork with other platforms. Standards containing unified and general concepts should be developed to accomplish interoperability among several IoT platforms. To achieve this goal, several standards have been developed and shared among de jure and de facto standards organizations (e.g., ISO/IEC 20922:2016 with MQTT and ISO/IEC 30118-1:2018 with OCF Core Specification). Furthermore, cooperation between standards organizations, academia, and industry is required for interoperability between divergent IoT platforms.

I. Comparison Between IoT Architectures

As described earlier, each standard organization defines an IoT architecture from its own perspectives, that is, with different goals. Herein, we compare various architectures. Table IV shows the comparison results. In particular, architectures with the same aspects are based on the IoT definition of an infrastructure of interconnected entities, people system, and information resources including service [1].

ISO/IEC provided a general-purpose IoT reference model in ISO/IEC 21823-1:2019 [95]. Its characteristics are influenced by the interaction between several entities, rather than by other architectures. These interactions may generate several opt for different IoT services or entities, but security-related considerations may be complex because different access control, authentication, and authorization mechanisms are required for each interaction. ITU-T provides an IoT reference model in ITU-T Y.4000/Y.2060 [128], which consists of simple layers: application, service and application support, network, and device. However, unlike other architectures, the architecture model considers security and management capabilities for all layers. ITU-T also provides an architecture for WoT in ITU-T Y.4400/Y.2063 [129]. It can facilitate the development of a WoT-based IoT system. OCF presented an IoT architecture for the OCF framework in OCF-CS [167]. It is designed to develop an IoT system based on the OCF framework. It provides specific and practical content (e.g., using the CoAP protocol and CRUDN operations). Although oneM2M provides its functional architecture in TR-0057-V0.3.0 [198], the standard is not published (i.e., the standard is included in the fourth release; thus, this is a draft version provided for information only). We considered only published standards; hence, oneM2M-based architectures are excluded.

J. Security-Related Considerations in Standards

As described in Section VI, several standards provide general content for security (see the column "general" in Table III); moreover, they provide various considerations for developing secure IoT systems (e.g., credential types for protocols, signature algorithms between network process, and prevention of malicious attacks). However, most standards only provide considerations without detailed regulations, methods, or technologies. This is because it is important to develop secure IoT systems, but it is difficult to resolve security-related issues. Therefore, research that provides security solutions in each standard is required.

K. Conformance Test

After the development of standard-based interoperability and security-related methods (e.g., ontology, network protocols, and semantic messages), the results should be evaluated to demonstrate that these methods correctly follow and optimize international standards. Therefore, criteria are required to verify that the methods correctly construct standard

TABLE IV
COMPARISON BETWEEN IOT ARCHITECTURES

Standard	Goal	Entity (Layers)	Characteristics	Communication protocol	Domain / Platform
ISO/IEC 21823-1:2019 [95]	To provide IoT reference architecture	* User * IoT System * Access and Communication * Operation and Management * Application and Service * IoT Device * IoT gateway	* Interconnection among several enties	Not specified	General / Not specified
ITU-T Y.4000/Y.2060 [128]	To provide IoT reference model	* Application * Service and application support * Network * Device	* Consideration security capabilities in whole layers * Consideration management capabilities for whole layers	Not specified	General / Not specified
ITU-T Y.4400/Y.2063 [129]	To provide architecture for Web of Things	* Application * Web service (including mash-up, WoT, and composite WoT services) * WoT broker (including service and adaption) * Physical (including Device)	* Consideration Web based environments	Not specified	WoT / Not specified
OCF core specifications [167]	To provide IoT architecture for OCF framework	* Resource Model (including client, service, operation, role, resource, and entitiy) * Data protocol (including operation protocol, server protocol, and CoAP protocol)	* Practical contents to support developing IoT system	CoAP	OCF framework / IoTivity

specifications. This can be resolved using various methods. For example, test data construction research can be conducted to verify the developed methods. In addition, test platform-related research is required to automatically verify the results.

L. Software Development Process

Several standards provide high-level perspectives of IoT systems (e.g., platform, framework, and architecture), and thus they can be applied in the development of such systems. However, interoperability issues should be considered when IoT systems are developed with different standards. In addition, these high-level perspectives should be considered from the early stage to the end of the development processes. Therefore, an overview of the software development processes is required for combining different high-level perspectives. The development process should be compatible with different architectures, frameworks, and platforms. Furthermore, the development process should consider several security-related issues for secure integration.

M. Interoperability Between Standards

We analyzed international standards, and the results demonstrate that several of these standards have similar purposes (i.e., the columns in Tables II and III). In addition, various IoT systems are developed based on different standards; thus, research on effective interworking among IoT standards is required to accomplish interoperability. Furthermore, research on the interoperability of standards may facilitate the integration of existing and developed IoT systems.

N. Data Sharing

Data sharing is the most important issue in IoT, and previous research has addressed this. However, herein, we consider data sharing in relation to international standards and standardization processes. A dictionary of resource definitions is required for unified meanings between IoT entities, and this should be provided as an international standard because systematic data definitions (e.g., name, range, measurement, and unit) are critical for proper data sharing. Moreover, an open framework is required to support spontaneous participation for standardization. By defining the dictionary, data exchange is possible between different IoT entities without data loss. In addition, this dictionary may enable ontologies, which may help assign new meanings to heterogeneous data.

O. Interworking With ICT Standards

IoT can be applied to and cooperate with various ICTs (e.g., cloud computing, blockchain, and edge/fog computing), and ICT has been standardized by international standards organizations. For example, blockchain standards have been developed in ISO/TC 307 [199] and IEEE-SA [200], and 5G network standards are being developed by 3GPP [201]. In addition, cloud and edge computing standards are being developed by ISO/IEC [202]. To accomplish effective interworking between IoT and ICT, research should be conducted on interworking methods between the corresponding IoT and ICT standards. These methods may facilitate the integration of IoT and various ICTs.

VIII. CONCLUSION

IoT has recently been studied, and divergent ICT fields have emerged; however, there are barriers for adaptation to IoT, namely, interoperability and security. Therefore, not only research groups but also standard organizations are actively researching how to overcome these barriers. Further, international standards may be a general solution for interoperability

and security. However, studies related to interoperability and security standards have not been previously reported in the literature. To solve this limitation, in this paper, we performed an international standards survey for interoperability and security in the IoT. In addition, international standard organizations developing IoT-related standards have also been surveyed to guide the investigation of standards. A systematic literature review process was conducted for the survey, and 183 international standards were searched. Finally, 67 standards related to interoperability and security were selected and analyzed. In addition, we performed a discussion and presented open research problems in IoT interoperability and security. To the best of our knowledge, this survey is the first to provide a deeper summary of international IoT standards for interoperability and security, and we are certain that the results can be useful to researchers. Our findings can be summarized as follows:

- Several interoperability standards consider security, and vice versa.
- Some standards consider the same interoperability and security factors from different perspectives.
- Applying interoperability-related standards may aid in accomplishing interoperability if different IoT systems are developed using the same standard, that is, interoperability cannot be achieved by simply applying a standard.
- Interworking and interoperability are required among standards to accomplish standard-based security and interoperability in IoT systems.
- Several standards provide security-related considerations for various factors (e.g., platform, architecture, framework, and reference model), but not detailed methods.
- A more detailed analysis of existing research on standards is required to enhance IoT-related standards for interoperability and security.

In the future, we will continue this survey. First, we will survey studies that apply international standards. Furthermore, we intend to find various ICT-related standards that can be applied to IoT environments.

REFERENCES

[1] *Information Technology—Internet of Things (IoT)—Vocabulary*, International Organization for Standardization Standard ISO/IEC 20924:2021, Dec. 2018.

[2] Bain & Company. *Us Industrials Confront Implementation Barriers to the IoT*. Accessed: Mar. 25, 2020. [Online]. Available: https://www.bain.com/insights/us-industrials-confront-implementation-barriers-to-the-iot-snap-chart/

[3] L.-O. M. Walker, N. Jones, and L. Wallin, *How to Address the Top Five IoT Challenges With Enterprise Architecture*, Gartner. Inc., Stamford, CT, USA, 2016.

[4] J. Hahn, "The Internet of Things (IoT) and libraries," *Library Technol. Rep.*, vol. 53, no. 1, pp. 5–8, 2017.

[5] *New European Consortium to Improve IoT Security, Interoperability*. Accessed: Jan. 27, 2021. [Online]. Available: https://internetofbusiness.com/european-consortium-looks-to-improve-iot-interoperability-and-security/

[6] S. T. Demirel, M. Demirel, I. Dogru, and R. Das, "Interopt: A new testing platform based on onem2m standards for IoT systems," in *Proc. Int. Symp. Netw. Comput. Commun. (ISNCC)*, 2019, pp. 1–6.

[7] J. Hwang, A. Aziz, N. Sung, A. Ahmad, F. Le Gall, and J. Song, "Autocon-IoT: Automated and scalable online conformance testing for IoT applications," *IEEE Access*, vol. 8, pp. 43111–43121, 2020.

[8] A. Ahmed, M. Kleiner, and L. Roucoules, "Model-based interoperability iot hub for the supervision of smart gas distribution networks," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1526–1533, Jun. 2019.

[9] J. An *et al.*, "Toward global IoT-enabled smart cities interworking using adaptive semantic adapter," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5753–5765, Jun. 2019.

[10] E. Kovacs, M. Bauer, J. Kim, J. Yun, F. Le Gall, and M. Zhao, "Standards-based worldwide semantic interoperability for IoT," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 40–46, Dec. 2016.

[11] M. Schneider, B. Hippchen, S. Abeck, M. Jacoby, and R. Herzog, "Enabling IoT platform interoperability using a systematic development approach by example," in *Proc. Global Internet Things Summit (GIoTS)*, 2018, pp. 1–6.

[12] S.-Y. Ge, S.-M. Chun, H.-S. Kim, and J.-T. Park, "Design and implementation of interoperable IoT healthcare system based on international standards," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2016, pp. 119–124.

[13] B. Oryema, H.-S. Kim, W. Li, and J. T. Park, "Design and implementation of an interoperable messaging system for IoT healthcare services," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2017, pp. 45–52.

[14] G. Bouloukakis, N. Georgantas, P. Ntumba, and V. Issarny, "Automated synthesis of mediators for middleware-layer protocol interoperability in the IoT," *Future Gener. Comput. Syst.*, vol. 101, pp. 1271–1294, Dec. 2019.

[15] A. E. Khaled and S. Helal, "Interoperable communication framework for bridging restful and topic-based communication in IoT," *Future Gener. Comput. Syst.*, vol. 92, pp. 628–643, Mar. 19.

[16] J. Kim *et al.*, "Standard-based IoT platforms interworking: Implementation, experiences, and lessons learned," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 48–54, Jul. 2016.

[17] J. Yun, I.-Y. Ahn, N.-M. Sung, and J. Kim, "A device software platform for consumer electronics based on the Internet of Things," *IEEE Trans. Consum. Electron.*,' vol. 61, no. 4, pp. 564–571, Nov. 2015.

[18] O. Novo and M. D. Francesco, "Semantic interoperability in the IoT: Extending the Web of things architecture," *ACM Trans. Internet Things*, vol. 1, no. 1, pp. 1–25, 2020.

[19] S.-R. Oh and Y.-G. Kim, "Development of IoT security component for interoperability," in *Proc. 13th Int. Comput. Eng. Conf. (ICENCO)*, 2017, pp. 41–44.

[20] P. Matoušek, O. Ryšavỳ, and M. Grégr, "Security monitoring of iot communication using flows," in *Proc. 6th Conf. Eng. Comput. Based Syst.*, 2019, pp. 1–9.

[21] N. Y. Parotkin and V. V. Zolotarev, "Information security of IoT wireless segment," in *Proc. Global Smart Ind. Conf. (GloSIC)*, 2018, pp. 1–7.

[22] D. Adrianto and F. J. Lin, "Analysis of security protocols and corresponding cipher suites in ETSI M2M standards," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, 2015, pp. 777–782.

[23] K. Zandberg, K. Schleiser, F. Acosta, H. Tschofenig, and E. Baccelli, "Secure firmware updates for constrained iot devices using open standards: A reality check," *IEEE Access*, vol. 7, pp. 71907–71920, 2019.

[24] C. Lee, L. Nkenyereye, N. Sung, and J. Song, "Towards a blockchain-enabled IoT platform using oneM2M standards," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, 2018, pp. 97–102.

[25] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in Internet of Things: Taxonomies and open challenges," *Mobile Netw. Appl.*, vol. 24, no. 3, pp. 796–809, 2019.

[26] B. Di Martino, M. Rak, M. Ficco, A. Esposito, S. Maisto, and S. Nacchia, "Internet of Things reference architectures, security and interoperability: A survey," *Internet of Things*, vols. 1–2, pp. 99–112, Sep. 2018.

[27] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.

[28] H. R. Ghorbani and M. H. Ahmadzadegan, "Security challenges in Internet of things: Survey," in *Proc. IEEE Conf. Wireless Sens. (ICWiSe)*, 2017, pp. 1–6.

[29] D. M. Mena, I. Papapanagiotou, and B. Yang, "Internet of Things: Survey on security," *Inf. Security J. A Global Perspective*, vol. 27, no. 3, pp. 162–182, 2018.

[30] J.-Y. Yu, E. Lee, S.-R. Oh, Y.-D. Seo, and Y.-G. Kim, "A survey on security requirements for WSNs: Focusing on the characteristics related to security," *IEEE Access*, vol. 8, pp. 45304–45324, 2020.

[31] A. Oracevic, S. Dilek, and S. Ozdemir, "Security in Internet of Things: A survey," in *Proc. Int. Symp. Netw. Comput. Commun. (ISNCC)*, 2017, pp. 1–6.

[32] A. Gyrard, S. K. Datta, and C. Bonnet, "A survey and analysis of ontology-based software tools for semantic interoperability in IoT and WoT landscapes," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, 2018, pp. 86–91.

[33] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[34] I. Hwang and Y.-G. Kim, "Analysis of security standardization for the Internet of things," in *Proc. Int. Conf. Platform Technology Service (PlatCon)*, 2017, pp. 1–6.

[35] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, U.K., Keele Univ.*, vol. 33, no. 2004, pp. 1–26, 2004.

[36] *Welcome to TTA - Telecommunications Technology Association of Korea*. Accessed: Aug. 6, 2020. [Online]. Available: http://www.tta.or.kr/eng/index.jsp/

[37] *Cambridge English Dictionary: Meanings & Definitions*. Accessed: Mar. 25, 2020. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/

[38] *IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-2012 (Revision of IEEE Std 802.11-2007), pp. 1–2793, 2012.

[39] *The Constrained Application Protocol (COAP)*, IETF, RFC 7252, Jun. 2014.

[40] *The Websocket Protocol*, IEFT, RFC 6455, Dec. 2011.

[41] International Organization for Standardization, *Information Technology — Vocabulary*, ISO/IEC Standard ISO/IEC 2382:2015, Mar. 2015.

[42] Bain & Company. *Global Management Consulting Firm*. Accessed: Jul. 22, 2020. [Online]. Available: https://www.bain.com/

[43] Bain & Company. *Internet of Things Research / Business Insights*. Accessed: Jul. 22, 2020. [Online]. Available: https://www.bain.com/insights/topics/internet-of-things/

[44] Bain & Company. *How Providers Can Succeed in the Internet of Things*. Accessed: Jul. 22, 2020. [Online]. Available: https://www.bain.com/insights/how-providers-can-succeed-in-the-internet-of-things/

[45] Bain & Company. *What's Keeping Enterprise Customers From Adopting IoT Technology*. Accessed: Jul. 22, 2020. [Online]. Available: https://www.bain.com/insights/whats-keeping-enterprise-customers-from-adopting-IoT-technology-snap-chart/

[46] Bain & Company. *Us Industrials Confront Implementation Barriers to the IoT*. Accessed: Jul. 22, 2020. [Online]. Available: https://www.bain.com/insights/whats-keeping-enterprise-customers-from-adopting-IoT-technology-snap-chart/

[47] *Gartner*. Accessed: Jan. 27, 2021. [Online]. Available: https://www.gartner.com/

[48] *Home—Brain-IoT*. Accessed: Jan. 27, 2021. [Online]. Available: http://www.brain-iot.eu

[49] F. Burzlaff, N. Wilken, C. Bartelt, and H. Stuckenschmidt, "Semantic interoperability methods for smart service systems: A survey," *IEEE Trans. Eng. Manag.*, early access, Jul. 19, 2019, doi: 10.1109/TEM.2019.2922103.

[50] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[51] M. Elkhodr, S. Shahrestani, and H. Cheung, "The Internet of Things: New interoperability, management and security challenges," 2016. [Online]. Available: arXiv:1604.04824.

[52] Md. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the Internet of Things," in *Proc. IEEE World Congr. Services*, 2015, pp. 21–28.

[53] G. Kambourakis, C. Kolias, D. Geneiatakis, G. Karopoulos, G. M. Makrakis, and I. Kounelis, "A state-of-the-art review on the security of mainstream IoT wireless PAN protocol stacks," *Symmetry*, vol. 12, no. 4, p. 579, 2020.

[54] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696, Jun. 2020.

[55] M. Ganzha, M. Paprzycki, W. Pawłowski, P. Szmeja, and K. Wasielewska, "Semantic interoperability in the Internet of Things: An overview from the inter-IoT perspective," *J. Netw. Comput. Appl.*, vol. 81, pp. 111–124, Mar. 2017.

[56] J. Hou, L. Qu, and W. Shi, "A survey on Internet of Things security from data perspectives," *Comput. Netw.*, vol. 148, pp. 295–306, Jan. 2019.

[57] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[58] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[59] *Semantic Sensor Network Ontology*. Accessed: Mar. 25, 2020. [Online]. Available: https://www.w3.org/2005/Incubator/ssn/ssnx/ssn

[60] *Web of Things (WoT) Thing Description*. Accessed: Mar. 25, 2020. [Online]. Available: https://www.w3.org/TR/wot-thing-description/D142

[61] *GeoSPARQL–A Geographic Query Language for RDF Data*. Accessed: Mar. 25, 2020. [Online]. Available: https://www.ogc.org/standards/geosparql/#

[62] Open Connectivity Foundation, *OCF Resource to BLE Mapping Specification (Version 2.1.0)*, OCF Standard, Nov. 2019.

[63] Open Connectivity Foundation, *OCF Resource to Z-Wave Mapping Specification (Version 2.1.0)*, OCF Standard, Nov. 2019.

[64] Open Connectivity Foundation, *OCF Resource to Zigbee Cluster Mapping Specification (Version 2.1.0)*, OCF Standard, Nov. 2019.

[65] *IEEE Standard for Low-Rate Wireless Networks*, IEEE Standard 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011), pp. 1–709, 2016.

[66] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC Sublayer*, IEEE Standard 802.15.4e-2012 (Amendment to IEEE Std 802.15.4-2011), pp. 1–225, 2012.

[67] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 2: Active Radio Frequency Identification (RFID) System Physical Layer (PHY)*, IEEE Standard 802.15.4f-2012 (Amendment to IEEE Std 802.15.4-2011), pp. 1–72, 2012.

[68] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks*, IEEE Standard 802.15.4g-2012 (Amendment to IEEE Std 802.15.4-2011), pp. 1–252, 2012.

[69] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 4: Alternative Physical Layer Extension to Support Medical Body Area Network (MBAN) Services Operating in the 2360 MHz–2400 MHz Band*, IEEE Standard 802.15.4j-2013 (Amendment to IEEE Std 802.15.4-2011 as amended by IEEE Std 802.15.4e-2012, IEEE Std 802.15.4f-2012, and IEEE Std 802.15.4g-2012), pp. 1–24, 2013.

[70] *Inter-IoT—Interoperability Internet of Things*. Accessed: Jul. 13, 2020. [Online]. Available: https://inter-iot.eu/

[71] *ISO—Store*. Accessed: Mar. 25, 2020. [Online]. Available: https://www.iso.org/store.html

[72] *IEEE Xplore Digital Library*. Accessed: Mar. 25, 2020. [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp

[73] *ITU Telecommunication Standardization Sector*. Accessed: Mar. 25, 2020. [Online]. Available: https://www.itu.int/en/ITU-T/Pages/default.aspx

[74] *oneM2M–Home*. Accessed: Mar. 25, 2020. [Online]. Available: http://www.onem2m.org/

[75] *IETF | Internet Standards*. Accessed: Mar. 25, 2020. [Online]. Available: https://ietf.org/standards/

[76] *Open Connectivity Foundation (OCF)*. Accessed: Mar. 25, 2020. [Online]. Available: https://openconnectivity.org/

[77] *ISO/IEC JCT 1*. Accessed: Mar. 25, 2020. [Online]. Available: https://jtc1info.org/

[78] *Information Technology—Data Structure—Unique Identification for the Internet of Things*, ISO/IEC Standard ISO/IEC 29161:2016, Aug. 2016.

[79] *ISO—ISO/IEC CD 27030—Information Technology–Security Techniques–Guidelines for Security and Privacy in Internet of Things (IoT)*. Accessed: Mar. 25, 2020. [Online]. Available: https://www.iso.org/standard/44373.html

[80] *Information Technology—Future Network–Problem Statement and Requirements—Part 9: Networking of Everything*, ISO Standard TR 29181-9:2017, Apr. 2017.

[81] *Software, Systems and Enterprise—Architecture Evaluation Framework*, ISO/IEC/IEEE Standard 42030:2019, Jul. 2019.

[82] *IEEE SA—The IEEE Standards Association—Home*. Accessed: Mar. 25, 2020. [Online]. Available: https://standards.ieee.org/

[83] *P2413 WG*. Accessed: Mar. 25, 2020. [Online]. Available: http://grouper.ieee.org/groups/2413/

[84] *IEEE SA–Internet of Things Related Standards*. Accessed: Mar. 25, 2020. [Online]. Available: https://standards.ieee.org/initiatives/iot/stds.html

[85] *IEEE SA–Internet of Things Related Standards in Development*. Accessed: Mar. 25, 2020. [Online]. Available: https://standards.ieee.org/initiatives/iot/projects.html

[86] *ITU: Committed to Connecting the World*. Accessed: Mar. 25, 2020. [Online]. Available: https://www.itu.int/

[87] *IETF | Internet Engineering Task Force*. Accessed: Mar. 25, 2020. [Online]. Available: https://ietf.org/

[88] *Internet of Things Directorate (IoTDIR)—Review Requests*. Accessed: Mar. 25, 2020. [Online]. Available: https://datatracker.ietf.org/group/iotdir/reviews/

[89] *Reducing the Standards Track to Two Maturity Levels*, IETF, RFC 6410, Oct. 2011.

[90] *The Internet Standards Process—Revision 3*. IETF, RFC 2026, Oct. 1996.

[91] *Internet Research Task Force*. Accessed: Mar. 25, 2020. [Online]. Available: https://irtf.org/

[92] *Thing-to-Thing Research Group*. Accessed: Mar. 25, 2020. [Online]. Available: https://irtf.org/t2trg

[93] *oneM2M—Release 3*. Accessed: Mar. 25, 2020. [Online]. Available: http://www.onem2m.org/technical/published-drafts/release-3

[94] *Home | IoTivity*. Accessed: Mar. 25, 2020. [Online]. Available: https://iotivity.org/

[95] *Internet of Things (IoT)—Interoperability for Internet of Things Systems—Part 1: Framework*, ISO/IEC Standard ISO/IEC 21823-1:2019, Feb. 2019.

[96] *Internet of Things (IoT)—Reference Architecture*, ISO/IEC Standard ISO/IEC 30141:2018, Aug. 2018.

[97] *Information Technology—Internet of Things (IoT) Use Cases*, ISO/IEC Standard ISO/IEC TR 22417:2017, Nov. 2017.

[98] *Information Technology–Message Queuing Telemetry Transport (MQTT) v3.1.1*, ISO/IEC Standard ISO/IEC 20922:2016, Jun. 2016.

[99] G. Brown and L.-P. Lamoureux, "MQTT and the NIST cybersecurity framework version 1.0," OASIS Committee Note 01, OASIS, Burlington, MA, USA, 2014.

[100] A. Banks, E. Briggs, K. Borgendale, and R. Gupta, *MQTT Version 5.0*, OASIS Standard, 2019.

[101] D. K. McCormick, "802.11ba battery life improvement—Preview: IEEE technology report on wake-up radio," 2017, pp. 1–11, doi: 10.1109/IEEESTD.2017.8053470.

[102] *Information Technology—Radio Frequency Identification for Item Management—Part 1: Reference Architecture and Definition of Parameters to be Standardized*, ISO/IEC Standard ISO/IEC 18000-1:2008, Jul. 2008.

[103] *Information Technology—Radio Frequency Identification for Item Management—Part 2: Parameters for Air Interface Communications Below 135 KHz*, ISO/IEC Standard ISO/IEC 18000-2:2009, Oct. 2009.

[104] *Information Technology—Radio Frequency Identification for Item Management—Part 3: Parameters for Air Interface Communications at 13,56 MHz*, ISO/IEC Standard ISO/IEC 18000-3:2010, Nov. 2010.

[105] *Information Technology—Radio Frequency Identification for Item Management—Part 4: Parameters for Air Interface Communications at 2,45 GHz*, ISO/IEC Standard ISO/IEC 18000-4:2018, Aug. 2018.

[106] *Information Technology—Radio Frequency Identification for Item Management—Part 6: Parameters for Air Interface Communications at 860 MHz to 960 MHz General*, ISO/IEC Standard ISO/IEC 18000-6:2013, Jan. 2013.

[107] *Information Technology—Radio Frequency Identification for Item Management—Part 61: Parameters for Air Interface Communications at 860 MHz to 960 MHz Type A*, ISO/IEC Standard ISO/IEC 18000-61:2012, Jul. 2012.

[108] *Radio Frequency Identification for Item Management—Part 62: Parameters for Air Interface Communications at 860 MHz to 960 MHz Type B*, ISO/IEC Standard ISO/IEC 18000-62:2012, Jul. 2012.

[109] *Information Technology—Radio Frequency Identification for Item Management—Part 63: Parameters for Air Interface Communications at 860 MHz to 960 MHz Type C*, ISO/IEC Standard ISO/IEC 18000-63:2015, Oct. 2015.

[110] *Information Technology—Radio Frequency Identification for Item Management—Part 64: Parameters for Air Interface Communications at 860 MHz to 960 MHz Type D*, ISO/IEC Standard ISO/IEC 18000-64:2012, Jul. 2012.

[111] *Information Technology—Radio Frequency Identification for Item Management—Part 7: Parameters for Active Air Interface Communications at 433 MHz*, ISO/IEC Standard ISO/IEC 18000-7:2014, Sep. 2014.

[112] *Information Technology—Open Connectivity Foundation (OCF) Specification—Part 1: Core Specification*, ISO/IEC Standard ISO/IEC 30118-1:2018, Nov. 2018.

[113] *IEEE Standard for Information Technology—Local and Metropolitan Area Networks—Specific Requirements—Part 15.1A: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPAN)*, IEEE Standard 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002), pp. 1–700, 2005.

[114] *IEEE Standard for High Data Rate Wireless Multi-Media Networks*, IEEE Standard 802.15.3-2016 (Revision of IEEE Std 802.15.3-2003), pp. 1–510, 2016.

[115] *IEEE Recommended Practice for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 15.5: Mesh Topology Capability in Wireless Personal Area Networks (WPANS)*, IEEE Standard 802.15.5-2009, pp. 1–166, 2009.

[116] "Ieee standard for local and metropolitan area networks - part 15.6: Wireless body area networks," *IEEE Std 802.15.6-2012*, pp. 1–271, 2012.

[117] *IEEE Standard for Air Interface for Broadband Wireless Access Systems*, IEEE Standard 802.16-2012 (Revision of IEEE Std 802.16-2009), pp. 1–2542, 2012.

[118] *IEEE Standard for Air Interface for Broadband Wireless Access Systems—Amendment 1: Enhancements to Support Machine-to-Machine Applications*, IEEE Standard 802.16p-2012 (Amendment to IEEE Std 802.16-2012), pp. 1–82, 2012.

[119] *IEEE Standard for Wirelessman-Advanced Air Interface for Broadband Wireless Access Systems Amendment 1: Enhancements to Support Machine-to-Machine Applications*, IEEE Standard 802.16.1b-2012 (Amendment to IEEE Std 802.16.1-2012), pp. 1–126, 2012.

[120] *IEEE 802.11, The Working Group Setting the Standards for Wireless LANs*. Accessed: Mar. 25, 2020. [Online]. Available: http://www.ieee802.org/11/

[121] *Wi-Fi Alliance*. Accessed: Mar. 25, 2020. [Online]. Available: https://www.wi-fi.org/

[122] *IEEE Guide for Wireless Access in Vehicular Environments (Wave) Architecture*, IEEE Standard 1609.0-2019 (Revision of IEEE Std 1609.0-2013), pp. 1–106, 2019.

[123] *IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*, IEEE Standard 1609.2-2016 (Revision of IEEE Std 1609.2-2013), pp. 1–240, 2016.

[124] *IEEE Standard for Wireless Access in Vehicular Environments (Wave)—Networking Services Corrigendum 1: Miscellaneous Corrections*, IEEE Standard 1609.3-2010/Cor 1-2012 (Corrigendum to IEEE Std 1609.3-2010), pp. 1–19, 2012.

[125] *IEEE Standard for Wireless Access in Vehicular Environments (Wave)—Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)*, IEEE Standard 1609.11-2010, pp. 1–62, 2011.

[126] *IEEE Standard for Wireless Access in Vehicular Environments (Wave)—Identifiers*, IEEE Standard 1609.12-2019 (Revision of IEEE Std 1609.12-2016), pp. 1–17, 2019.

[127] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-2016 (Revision of IEEE Std 802.11-2012), pp. 1–3534, 2016.

[128] *Overview of the Internet of Things*, ITU-T Standard ITU-T Y.4000/Y.2060, Jun. 2012.

[129] *Framework of the Web of Things*, ITU-T Standard ITU-T Y.4400/Y.2063, Jun. 2012.

[130] *Functional Framework and Capabilities of the Internet of Things*, ITU-T Standard ITU-T Y.2068, Mar. 2015.
[131] *Common Requirements and Capabilities of a Gateway for Internet of Things Applications*, ITU-T Standard ITU-T Y.4101/Y.2067, Oct. 2017.
[132] *Common Requirements and Capabilities of Device Management in the Internet of Things*, ITU-T Standard ITU-T Y.4702, Mar. 2016.
[133] *Requirements of Smartphone as Sink Node for IoT Applications and Services*, ITU-T Standard ITU-T Y.4553, Mar. 2016.
[134] *Requirements of the Plug and Play Capability of the Internet of Things*, ITU-T Standard ITU-T Y.4112/Y,2077, Feb. 2016.
[135] *Semantics Based Requirements and Framework of the Internet of Things*, ITU-T Standard ITU-T Y.4111/Y.2076, Feb. 2016.
[136] *OID-Based Resolution Framework for Heterogeneous Identifiers and Locators*, ITU-T Standard ITU-T X.675, May 2015.
[137] *Coap (Constrained Application Protocol) Over TCP, TLS, and Websockets*, IETF, RFC 8323, Feb. 2018.
[138] *Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things*, IETF, RFC 7925, Jul. 2016.
[139] *The Transport Layer Security (TLS) Protocol Version 1.2*, IETF, RFC 5246, Aug. 2008.
[140] *Datagram Transport Layer Security Version 1.2*, IETF, RFC 7925, Jan. 2012.
[141] *Internet of Things (IoT) Security: State of the Art and Challenges*, IETF, RFC 8576, Apr. 2019.
[142] *Energy-Efficient Features of Internet of Things Protocols*, IETF, RFC 8352, Apr. 2018.
[143] *Report From the Internet of Things (IoT) Semantic Interoperability (IoTSI) Workshop 2016*, IETF, RFC 8477, Oct. 2018.
[144] *Security Solutions*, oneM2M Standard TS-0003-V3.11.0, Dec. 2019.
[145] *Secure Environment Abstraction*, oneM2M Standard TS-0016-V3.0.2, Apr. 2019.
[146] *Service Layer Core Protocol*, oneM2M Standard TS-0004-V3.15.0, Jan. 2020.
[147] *Coap Protocol Binding*, oneM2M Standard TS-0008-V.3.5.0, Oct. 2019.
[148] *HTTP Protocol Binding*, oneM2M Standard TS-0009-V3.5.0, Oct. 2019.
[149] *MQTT Protocol Binding*, oneM2M Standard TR-0010-V3.0.1, Mar. 2019.
[150] *Websocket Protocol Binding*, oneM2M Standard TS-0020-V3.0.1, Feb. 2019.
[151] *Management Enablement (BBF)*, oneM2M Standard TS-0006-V3.6.2, Feb. 2019.
[152] *Ontology Documentation*. Accessed: Mar. 25, 2020. [Online]. Available: https://ontology.tno.nl/saref/
[153] *Semantics Support*, oneM2M Standard TS-0034-V3.0.2, Jun. 2019.
[154] *Home Appliances Information Model and Mapping*, oneM2M Standard TS-0023-V3.7.3, Apr. 2019.
[155] *Interworking Framework*, oneM2M Standard TR-0033-V3.0.0, Apr. 2019.
[156] *OCF Interworking*, oneM2M Standard TS-0024-V3.2.2, Apr. 2019.
[157] *3GPP Interworking*, oneM2M Standard TS-0026-V3.3.0, Nov. 2019.
[158] *Architecture Enhancements to Facilitate Communications With Packet Data Networks and Applications*, 3GPP Standard TS 23.682, Dec. 2019.
[159] *Developer Guide of 3GPP Interworking*, oneM2M Standard TS-0026-V3.3.0, Apr. 2018.
[160] *Ontology Based Interworking*, oneM2M Standard TS-0030-V3.0.2, Apr. 2019.
[161] *Base Ontology*, oneM2M Standard TS-0012-V3.7.3, Feb. 2019.
[162] *OSGI Interworking*, oneM2M Standard TS-0035-V3.0.0, Apr. 2019.
[163] *OSGI—Alliance—The Dynamic Module System for Java*. Accessed: Mar. 25, 2020. [Online]. Available: https://www.osgi.org/
[164] *Use Cases Collection*, oneM2M Standard TR-0001-V3.1.1, May 2019.
[165] *Industrial Domain Enablement*, oneM2M Standard TR-0018-V2.5.1, Jan. 2018.
[166] *OCF—Specifications*. Accessed: Mar. 25, 2020. [Online]. Available: https://openconnectivity.org/developer/specifications/
[167] Open Connectivity Foundation, *OCF Core Specification (Version 2.1.0)*, OCF Standard, Nov. 2019.
[168] Open Connectivity Foundation, *OCF Core—Optional Specification (Version 2.1.0)*, OCF Standard, Nov. 2019.
[169] Open Connectivity Foundation, *OCF Device Specification (Version 2.1.0)*, OCF Standard, Nov. 2019.
[170] Open Connectivity Foundation, *OCF Device to Cloud Services Specification (Version 2.1.0)*, OCF Standard, Nov. 2019.
[171] Open Connectivity Foundation, *OCF Bridging Specification (Version 2.1.0)*, OCF Standard, Nov. 2019.
[172] Open Connectivity Foundation, *OCF Resource Type Specification (Version 2.1.0)*, OCF Standard, Nov. 2019.
[173] Open Connectivity Foundation, *OCF Wi-Fi Easy Setup Specification (Version 2.1.0)*, OCF Standard, Nov. 2019.
[174] Open Connectivity Foundation, *OCF Resource to UPlus Mapping Specification (Version 2.1.0)*, OCF Standard, Nov. 2019.
[175] Open Connectivity Foundation, *OCF Resource to OneM2M Module Class Mapping Specification (Version 2.1.0)*, OCF Standard, Nov. 2019.
[176] Open Connectivity Foundation, *OCF Resource to AllJoyn Interface Mapping Specification (version 2.1.0)*, OCF Standard, Nov. 2019.
[177] *Information Technology—Open Connectivity Foundation (OCF) Specification—Part 2: Security Specification*, ISO/IEC Standard ISO/IEC 30118-2:2018, Nov. 2018.
[178] Open Connectivity Foundation, *OCF Cloud Security Specification (version 2.1.0)*, OCF Standard, Nov. 2019.
[179] S.-R. Oh, Y.-G. Kim, and S. Cho, "An interoperable access control framework for diverse IoT platforms based on oauth and role," *Sensors*, vol. 19, no. 8, p. 1884, 2019.
[180] S.-R. Oh and Y.-G. Kim, "AFaaS: Authorization framework as a service for Internet of Things based on interoperable OAuth," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 2, pp. 1–15, 2020, doi: 10.1007/s12652-019-01367-2.
[181] J. Koo and Y.-G. Kim, "Interoperability of device identification in heterogeneous IoT platforms," in *Proc. 13th Int. Comput. Eng. Conf. (ICENCO)*, 2017, pp. 26–29.
[182] J. Koo, S.-R. Oh, and Y.-G. Kim, "Device identification interoperability in heterogeneous IoT platforms," *Sensors*, vol. 19, no. 6, p. 1433, 2019.
[183] M. Salehie and L. Tahvildari, "Self-adaptive software: Landscape and research challenges," *ACM Trans. Auton. Adapt. Syst. (TAAS)*, vol. 4, no. 2, pp. 1–42, 2009.
[184] E. Lee, Y.-G. Kim, Y.-D. Seo, and D.-K. Baik, "Self-adaptive framework with game theoretic decision making for Internet of Things," in *Proc. TENCON IEEE Region 10 Conf.*, 2018, pp. 2092–2097.
[185] E. Lee, Y.-D. Seo, and Y.-G. Kim, "Self-adaptive framework based on mape loop for Internet of Things," *Sensors*, vol. 19, no. 13, p. 2996, 2019.
[186] E. Lee, Y.-D. Seo, and Y-.G. Kim, "A nash equilibrium based decision-making method for Internet of Things," *J. Ambient Intell. Humanized Comput.*, to be published, doi: 10.1007/s12652-019-01367-2.
[187] P. Arias-Cabarcos, C. Krupitzer, and C. Becker, "A survey on adaptive authentication," *ACM Comput. Surveys*, vol. 52, no. 4, pp. 1–30, 2019.
[188] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Advanced Communication Technology (ICACT)*, 2017, pp. 464–467.
[189] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[190] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proc. IEEE/ACM 2nd Int. Conf. Internet-of-Things Design Implement. (IoTDI)*, 2017, pp. 173–178.
[191] *Software*. Accessed: Aug. 6, 2020. [Online]. Available: http://mqtt.org/software/
[192] *Welcome to TTA—Telecommunications Technology Association of Korea*. Accessed: Aug. 6, 2020. [Online]. Available: https://www.onem2m.org/developer-guides
[193] *OneM2M*. Accessed: Aug. 6, 2020. [Online]. Available: https://wiki.onem2m.org/
[194] *oneM2M—Technical Questions*. Accessed: Aug. 6, 2020. [Online]. Available: https://www.onem2m.org/developers-corner/documentation/technical-questions
[195] *Projects–Explore–GitLab*. Accessed: Aug. 6, 2020. [Online]. Available: https://git.onem2m.org/explore/projects
[196] *oneM2M—Open Source Projects*. Accessed: Aug. 6, 2020. [Online]. Available: https://www.onem2m.org/developers-corner/tools/open-source-projects
[197] *oneM2M—App-ID Registry*. Accessed: Aug. 6, 2020. [Online]. Available: https://www.onem2m.org/developers-corner/tools/app-id-registry
[198] *Getting Started With oneM2M*, oneM2M Standard TR-0057-V0.3.0, May 2019.
[199] *ISO–ISO/TC 307—Blockchain and Distributed Ledger Technologies*. Accessed: Oct. 25, 2020. [Online]. Available: https://www.iso.org/committee/6266604/x/catalogue/
[200] *Standards—IEEE Blockchain Initiative*. Accessed: Oct. 25, 2020. [Online]. Available: https://blockchain.ieee.org/standards

[201] *3GPP Specification Set: 5G*. Accessed: Oct. 25, 2020. [Online]. Available: https://www.3gpp.org/dynareport/SpecList.htm?release=Rel-15&tech=4
[202] *ISO–35.210—Cloud Computing*. Accessed: Oct. 25, 2020. [Online]. Available: https://www.iso.org/ics/35.210/x/

Euijong Lee received the B.S. degree in computer information and science and the Ph.D. degree in computer science and engineering from Korea University, Seoul, South Korea, in 2012 and 2018, respectively. He was a Postdoctoral Researcher with the Department of Computer and Information Security, Sejong University. He is currently an Assistant Professor with the Department of Computer Science, Chungbuk National University, Cheongju, South Korea. His research interests include self-adaptive software, software engineering, model checking, Internet of Things, and data mining.

Young-Duk Seo received the B.S. degree in computer and communication engineering and the Ph.D. degree in computer science and engineering from Korea University, Seoul, Republic of Korea, in 2012 and 2018, respectively.

He was a Research Professor with the Computer, Information and Communication Research Institute, Korea University and a Postdoctoral Researcher with the Department of Computer and Information Security, Sejong University. He was an Assistant Professor with the Department of Data Science, Sejong University. He is currently an Assistant Professor with the Department of Computer Engineering, Inha University. His research interests include self-adaptive software, big data analysis, recommender system, and entity linking.

Se-Ra Oh received the B.E. degree in computer software from Dongyang Mirae University in 2016 and the Ph.D. degree in computer and information security from Sejong University in 2021. He has published more than ten research articles in the field of information security. His current research interests include the Internet of Things security and access control.

Young-Gab Kim (Member, IEEE) received the B.S. degree in biotechnology and genetic engineering and minored in computer science and engineering and the M.S. and Ph.D. degrees in computer science and engineering from Korea University, Seoul, South Korea, in 2001, 2003, and 2006 respectively. He was an Assistant Professor with the School of Information Technology, Catholic University of Daegu. He is currently an Associate Professor with the Department of Computer and Information Security, and Convergence Engineering for Intelligent Drone, Sejong University. He has published over 130 research papers in the field of computer science and information security. His current research interests include big data security, network security, home network, security risk analysis, and security engineering. As a Korean ISO/IEC JTC 1 member, he is contributing in developing data exchange standards.