J Inf Process Syst, Vol.15, No.4, pp.797~819, August 2019
https://doi.org/10.3745/JIPS.03.0125

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Comprehensive Survey on Internet of Things, Architecture, Security Aspects, Applications, Related Technologies, Economic Perspective, and Future Directions

Khusanbek Gafurov* and Tai-Myoung Chung*

Abstract

Internet of Things (IoT) is the paradigm of network of Internet-connected things as objects that constantly sense the physical world and share the data for further processing. At the core of IoT lies the early technology of radio frequency identification (RFID), which provides accurate location tracking of real-world objects. With its small size and convenience, RFID tags can be attached to everyday items such as books, clothes, furniture and the like as well as to animals, plants, and even humans. This phenomenon is the beginning of new applications and services for the industry and consumer market. IoT is regarded as a fourth industrial revolution because of its massive coverage of services around the world from smart homes to artificial intelligence-enabled smart driving cars, Internet-enabled medical equipment, etc. It is estimated that there will be several dozens of billions of IoT devices ready and operating until 2020 around the world. Despite the growing statistics, however, IoT has security vulnerabilities that must be addressed appropriately to avoid causing damage in the future. As such, we mention some fields of study as a future topic at the end of the survey. Consequently, in this comprehensive survey of IoT, we will cover the architecture of IoT with various layered models, security characteristics, potential applications, and related supporting technologies of IoT such as 5G, MEC, cloud, WSN, etc., including the economic perspective of IoT and its future directions.

Keywords

Cloud, Edge, IoT, IoT Security, MEC/MCC, RFID, WSN, 5G

1. Introduction

Internet of Things (IoT) is defined as the extension of Internet into real world objects wherein physical items are present both in real and virtual worlds and can be monitored remotely [1], according to Jie et al. [2]. It is an interconnection of massive devices in cyber space through data collection, sharing, and analysis in heterogeneous networks. The growth of IoT depends on advances in mobile devices, embedded and ubiquitous communication, cloud computing, and data analytics [3]. IoT provides services over the traditional Internet by enabling human-to-thing, thing-to-thing, or thing-to-things communications [4]. The pervasive presence of embedded systems around us with RFID tags, sensors, and actuators that can interconnect to each other to reach common goals is regarded as IoT [5-7].

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Manuscript received January 3, 2019; first revision April 10, 2019; accepted April 18, 2019.
Corresponding Author: Khusanbek Gafurov (x.gafurov@skku.edu)
* College of Information and Communication Engineering, Sungkyunkwan University, Suwon, Korea (x.gafurov@gmail.com, tmchung@skku.edu)

Copyright© 2019 KIPS

The term 'Internet of Things' originates from the supply chain management scenario [8] referred to by Kevin Ashton. Mr. Ashton, an assistant brand manager at P&G, proposed the application of RFID in the supply chain and later formed Auto-ID Lab at MIT [9]. Since then, many multinational organizations around the world have been participating in the development of IoT [10].

IoT has gone through further design changes over the course of its development period. The early scenario of IoT was a three-layer model with sensors and actuators as underlying layer, further covering the top of it as the cloud computing layer [8]. Service-oriented architecture (SOA) turned out to be the next applicable model to implement IoT [5]. The concept of SOA is as simple as a component-based model that can be constructed to connect numerous services through interfaces and protocols [11]. Recent studies show that the compatible and applicable model for IoT is considered to be CISCO's seven-layer model. The early report by CISCO describes the seven-layer model in detail with possible applications [12].

As we have mentioned in the abstract, and with many references raising the alarm [4,5], the security perspective in IoT must be considered seriously. Due to the lack of support for advanced cryptography mechanisms and low computational power, IoT devices are very vulnerable to security attacks [4]. The Denial of Service (DoS) attack is one of the common scenarios in the IoT threat case [13]. To provide a solid framework for Security, lists of requirements are proposed in the academe. Mosenia and Jha [4] proposed the combination of the CIA triad as confidentiality, integrity, and availability and IAS octave as accountability, auditability, trustworthiness, non-repudiation, and privacy to be compact security requirements.

Because of the miniaturization of the embedded computing devices and features of peer-to-peer networking and communication over the traditional Internet architecture, there are various application criteria to be proposed. Sensors and actuators, too, lay the foundation in the serviceability of IoT. The novel IoT application was started with a simple Coke vending machine [14] that already provided the features of checking the status such as coldness and availability of loaded cans. Furthermore, applications including Smart Grid, Smart Transportation, Smart Cities [2], smart buildings, health monitoring, energy management, construction management, environmental monitoring, production and assembly line management, and food supply chain [4] are regarded as potential IoT applications. The airline industry also applies the RFID baggage tracing mechanism [15] as well as the application of IoT in agriculture [16,17] and E-commerce services [18] in the paradigm of supermarkets have been provided.

Besides the applications of IoT and security specifications, various other supporting technologies of IoT need to be taken into account. For example, Cyber Physical Systems (CPS) are the integration of cyber and physical components through modern computing and communication technologies [19]; Cloud computing paradigm is also proposed in convergence with IoT [20], mobile edge computing (MEC), and mobile cloud computing (MCC) technologies composed of numerous edge side layer computing servers located at telecom towers or crowded spots near the end users, which handle the partial load of data preprocessing to ease the volume for the cloud and improve user content delivery access speed and bandwidth [21,22]. Direct mobile-to-mobile communication support with 5G technology [23], big data support for IoT [24], and machine learning for massive data preprocessing and security provisioning [25] will support IoT QoS efficiency, data integrity, and scalability.

The rest of this paper is organized as follows. In Section 2, we list and discuss related surveys, comprehensive studies on IoT, security, scalability, and other related materials that we found useful. We list the information in tabular format so that readers can have a critical overview and a comparison of the

found resources, and we refer to the state-of-the-art and cornerstone research works that are considered important in the academe and the industry. Next, in Section 3, we cover the state-of-the-art IoT and its development cycle with various figures and charts. We discuss the institutions and organizations working for the development of IoT as well as provide detailed discussion of the layered architecture of IoT from three-layer to seven-layer models, including the potential applications of IoT and existing research on it. Furthermore, we list the related technologies in every layer combined with IoT and also provide a short discussion of IoT economies of scale. Security is also one of the very important points in IoT, so we draw attention to the security aspects in Section 4 and current research on this area, and what countermeasures are implemented and published will be covered. In addition, we mention briefly the several frameworks of IoT security and role of cryptography in the construction of defense mechanisms for IoT security. Next, we provide the future topics and directions. The conclusion and acknowledgment are presented in the next sections.

2. Related Work

There are various existing surveys, and research has been carried out in the academe. Note, however, that finding out about all these materials and resources will take a tremendous amount of research time. To make it easy for newcomers in the IoT field and to give comprehensive information about the diverse areas of IoT we dedicate this section for other existing related surveys, literature, and research works of many other popular authors so that readers can quickly switch to other works and get more detailed information. In other words, with this single survey paper, we try to accomplish one paper access to the entire IoT field.

To make information clear and concise, we have set up tabular information by putting the citations to the survey and research papers of various mostly cited papers in periodical format. Research and survey papers that came out from year 2000 up to the current time were considered. We set two different categories for the material: research and survey. We also reviewed existing materials in the six main fields: IoT, IoT security, fog/edge and cloud computing, CPS, and MEC/MCC.

According to Table 1, most of the survey works came out during the period 2005–2015 that we just labeled as 2010. It emphasizes that interest in the IoT field has drastically improved during this period, as a result of which more survey papers were written and published in the next several years until the current time of 2018. There were new survey papers published within the current time. In the field of IoT Security in particular, a distinct number of survey papers were published until 2018.

In addition, edge computing as a side support for cloud computing has been the recent trend to date. As a result, more researchers are getting into this field, and there are many comprehensive research papers published for the last two years. We believe that edge computing might be a possible future study topic. CPS and MEC/MCC are also important support technologies in the entire paradigm of IoT, so interest in this field is growing, possibly giving rise to new survey and research papers in the coming years.

Meanwhile, there are obviously far more papers available in the academe, and we might not cover all of them. Thus, we tried to select the papers that we found to be valuable and the survey papers we gathered, each fifteen pages long on average. One of the most valuable papers we considered is the one by Lin et al. [2] and Al-Fuqaha et al. [30] as it provides a comprehensive survey on the entire IoT paradigm, covering all the important aspects such as IoT architecture, various network protocols, integration of fog

Table 1. List of survey materials, literature, and research works in chronological order

Technology	2000		2010		2018	
	Type of work		Type of work		Type of work	
	Survey	Research	Survey	Research	Survey	Research
IoT	[26]	[58]	[5], [8], [9], [10], [11], [12], [20], [28], [30]	[31], [35]	[2], [3], [6], [7], [24], [25], [27], [29], [34], [36], [39]	[57]
IoT security	[51]		[33], [41], [42], [50], [56], [60]	[48], [49], [54]	[4], [7], [13], [37], [38]	[59]
Edge			[43], [44]	[55]	[21], [32]	[53]
Cloud		[47]	[20], [52]			[46]
CPS	[45]		[19], [40]	[19]	[2]	
MEC/MCC					[22]	

computing, security and privacy, variety of IoT services and applications, role of CPS within IoT, and potential market opportunities and elements of IoT. On the other hand, Mosenia and Jha [4] give more comprehensive information on IoT security by categorizing the topics into Edge nodes, communications, and edge computing. Authors also cover security threats and countermeasures of RFID tags in the paradigm of seven-layer IoT architecture.

In Fig. 1, we set up another visual illustration for the citations we gathered from Table 1. In this pie chart, we put the most important survey works divided into distinct categories of IoT, IoT security, edge, cloud, etc., and placed the most recent publications up to the current time at the center of the pie chart. The further located citations are survey papers published in the past, the further the citation from the center is, the older the publication year.

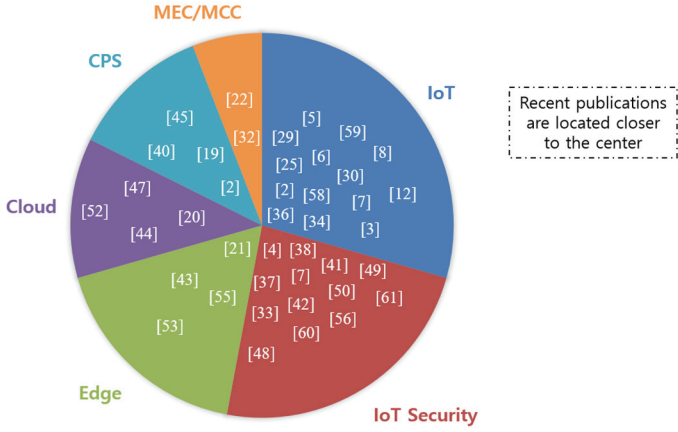

Fig. 1. Citations of existing survey papers in the industry categorized into research fields.

In fact, these are not all the existing survey and research papers that we were able to find in the academe. There are many works that we simply did not include in this survey, although they were decent works done by the authors, because they were not enough or comprehensive enough to cover many aspects of the IoT field. Nonetheless, we believe that the existing works we covered will be wide enough to give a

detailed overview of the IoT paradigm and to make it easy for the researchers to pick a niche field to work on and contribute their efforts.

Furthermore, we list interesting research works in the academe. The integration of IoT into medical health and lifelong personal health monitoring is observed broadly in the following research works [61]: insulin pump hijacking [62] and pacemaker security [63]; detection of sinkhole attacks [54]; Sybil attack prevention [51]; construction of smart cities [35]; potential applications of intrusion detection systems in IoT [33]; operating systems for IoT [28]; methods of analyzing big data [34] and applications of machine learning algorithms [25]. The research by Dao et al. [64] on DDoS attack behavior learning with the application of self-organizing maps (SOM) as a filter to detect DoS stream data and research work on the application of IoT in agriculture [16,17] happen to be several interesting research works that we also put in Table 1.

Furthermore, research efforts on various current IoT protocols [65] such as CoAP [66] and DDS [67] will be valuable. The survey work on wireless sensor networks (WSN) [68] also depicts further detailed information on IoT as the early three-layer model of IoT features the composition of WSN and other components. Survey and research works on smart city [35,69], threat of bot net composed with DDoS [70], research on body area network [71], side channel investigation through EM signal leak [72], and survey works on RFID [73,74] are the most cited and reviewed publications in the academe.

We have written this survey paper based on the existing recent publications that we have referred to in this section.

3. Status and Overview of IoT Development

Over the course of several decades, IoT has been developed to become the fourth industrial revolution [75]. There are many factors for the growth of IoT applications being widely used from our daily life to industrial fields. Two main factors can be credited for this: increase in the computation power and miniaturization of integrated circuit boards. In the following two sections, we describe the development of layered IoT architecture and the brief timeline of the history of IoT.

3.1 Development of IoT-Layered Architecture and Timeline

Fig. 2 shows the three different layered architectures of IoT. In Fig. 2, section (a) shows that the early IoT model was a three-layer architecture demonstrated by Gubbi et al. [8] in their research work. Basically, it consists of sensors and actuators as things in the ground layer, cloud as an information processing layer, as and application layer that allows interaction by users as the third layer.

Furthermore, [30] gives the definition of IoT architecture as middleware layer-based and SOA-based in their research work. For better understanding, we refer to the research by Atzori et al. [5] as a comprehensive study of the SOA-based five-layer model. As we can see from Fig. 2 section (b) layers are categorized into service composition and management as well as object abstraction. Meanwhile, the ground layer is considered to consist of objects.

Finally, the recent proposal for the IoT layered architecture is delivered by CISCO as a seven-layer model [12] as we can see in section c of Fig. 2. The previous SOA-based architecture was changed by adding a user and process layer and edge computing layer. In particular, edge computing is a new concept,

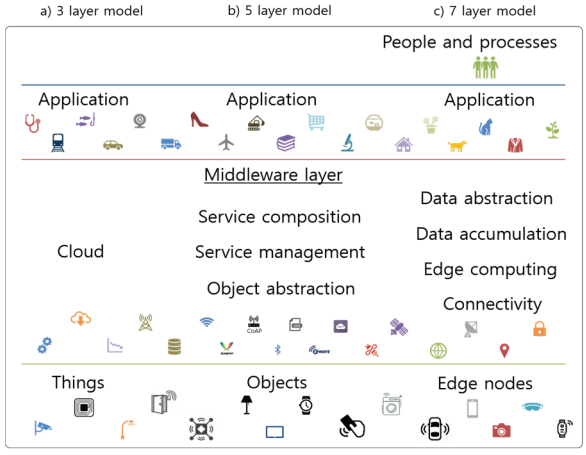

Fig. 2. Brief overview of three-, five-, and seven-layer IoT models.

and there are numerous surveys and research works in this field [21,22,32,53]. The concept of edge computing involves supporting cloud computing and providing better quality of service for end users. Edge computing will be discussed further in the later sections.

Additionally, there are several types of technologies in each layer. For example, the objects layer, also called perception layer, is supported by RFID, diverse types of sensors such as motion sensor, light, proximity, audio and temperature, barometer, etc., and even hobbyist users as well as the industry also use various open-sourced available circuit boards to build their IoT devices, such as Arduino, Phidgets, Intel Galileo, Raspberry pi [30], etc., Contiki, TinyOS, LiteOS, Riot OS, and Android are several operating systems designed for embedded systems and portable computing devices [30]. In addition, the network layer or connectivity layer is supported by several protocols and technologies such as Bluetooth, IEEE 802.15.4, Z-Wave, WiFi, LTE-A, DDS, and ZigBee [30].

The evolution of the Internet by the early project implemented by DARPA, called DARPANET, and intended to connect military units around the USA [2], gave a birth to many potential applications and services that we use these days; this implies that the background technologies are Internet. Note, however, that many other factors play a key role, too. One of them is obviously World Wide Web (WWW), and recently the IoT and all related technologies.

Table 2 presents the timeline of the IoT evolution to the fourth industrial revolution. As we can see, all the advances arose from the invention of RFID in the 1980s. In fact, technologies triggering the point for IoT came out far earlier than the 1980s, but we tried to cover only the period between the 80s and up to now, and a detailed survey on IoT history is beyond the scope of this survey research. Nonetheless, further information can be found by referring to the links we provided in Table 2. Furthermore, UPC's usage at the supermarket and Coke machine installation at Carnegie Melon University were further triggers for IoT.

In addition, Tim Berners Lee established the World Wide Web at CERN (Conseil Européen pour la Recherche Nucléaire) in 1991, serving as the foundation for building a society that is open to the world. Many new inventions were also born in the 90s. Nonetheless, most important among them is the mention of IoT for the first time by Kevin Ashton while working as adviser at P&G. At the same time, he established Auto-ID Lab at MIT. Although it was not successful enough, companies like Microsoft and Novel introduced their early IoT products, namely "at work" and "Nest", to the market.

Table 2. Timeline of IoT development

Period	Technology
1980s	Mario Cardullo patent for RFID [15], UPC used in supermarket [2], Coke machine at Carnegie Melon University [76], Steve Mann wearable PC [76]
1990s	Olivetti active badge system [76], Mark Weiser's famous paper [26], Xerox EuroPARC Forget-me-not wearable device enabling peer-to-peer communication, storing information in database [76], Steve Mann wearable wireless camera [76], M1-GSM data module for M2M [76], Early IEEE Symposium on Wearable Computers [76], Kevin Ashton used IoT for the first time at P&G and Auto-ID MIT established [76], Microsoft introduced Novel NEST at work [77]
2000s	Neil Gershenfeld's "When things start to think" paper [76], David Brock's The Electric Product Code (EPC) Auto-ID lab Technology 1 [76], G. Lawton's "Machine-to-machine technology gears up for growth" paper [76], Arduino developed by Interaction Design Institute Ivrea (IDII) [76], Google Incorporated [78], LG Electronics Internet Fridge [79], Wi-Fi [80], RFID Passport [80]
2010s	According to IBSG, IoT was born with more things connected than people [78], Xively IoT OS [79], Contiki, TinyOS [78] IPv6 public launch [78], iPhone and iPad introduction [77], Cellular Parking meter [80], Warehouse logistics [80], Self-driving car [80], 3D printing [80]
2018	Google Nest [80], Apple watch [36], heart pacemaker [4], Amazon Alexa [81], Kakao mini [82], 5G [23]

Similarly, the period of 2000s was a time of various important publications and different standardization establishments for IoT. At the end of 2000s, however, LG Electronics [79] introduced its first Internet-connected refrigerator that had novice skills of ordering specific groceries online and energy saving modes. Moreover, the introduction of Wi-Fi technology vastly improved the network bandwidth and, as a result, consumer demand for Internet connection. The integration of RFID chips by US-based companies and its adaptation in other developed and developing countries allowed safety and security for citizens.

The many advancements in data communication from 2012 up to the current time, such as the introduction of lightweight communication protocols including ZigBee and Z-Wave [2,4] and adaptation of IPv6 [78] and massive increase in CPU processing power according to Moore's Law, paved the way for the birth of many IoT products such as Google Nest, Apple smart phones, tablets, and watches, 5G communication technology, various categories of AI speakers, and even artificial heart pacemakers.

3.2 Comprehensive Outline of IoT Architecture

Application layer: This layer deals with various applications of IoT to different areas of our lives. Starting from Smart Homes, smart factories are also included. Due to massive changes in all aspects of society, IoT is mentioned as the fourth industrial revolution. Fig. 3 shows the potential types of IoT applications we have studied. There are further niches of other applications discussed in the publications, but we have selected the most relevant and important ones in our survey.

In addition, we set apart IoT application categories into medical industry, smart home environment, smart transportation, and smart environment such as smart city, smart shopping, and IoT-enabled manufacturing. In all these various applications, IoT is basically applied with several sensors, actuators, data analytics, and visualization instruments that allow IoT to be available anytime, anywhere and on any object.

The medical industry is one of the largest demanded areas in the entire IoT paradigm [30], and a large part of the market share of IoT belongs to this field. There are various start-ups and institutions initiated to deliver services and products to hospitals and for homes for monitoring patients [8,30].

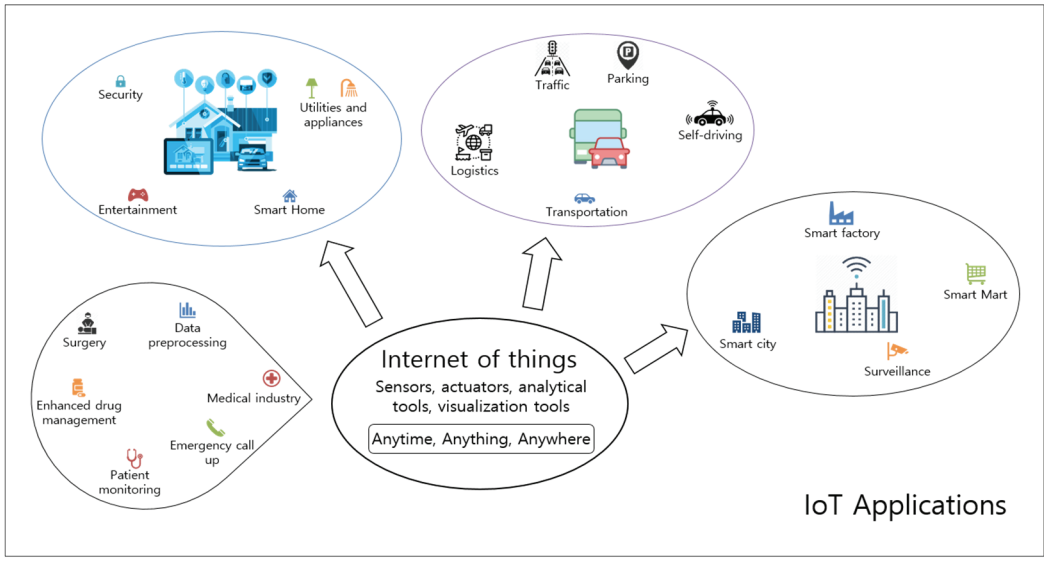

Fig. 3. IoT applications.

Various sensors are the foundational components of industrial IoT to provide both automation of processing and security. Note, however, that the automation of tasks and robotization may result in loss of jobs, which will not satisfy the government in terms of division of labor [8]. Meanwhile, new jobs are also created in design, modeling, and analytics of smart factories [83] as well as anything related to these directions.

Industrial IoT will ensure efficiency and effectiveness [84] in the management of product as well as manufacturing process maintenance. Meanwhile, IoT components can also be used for efficient energy management and effective monitoring of devices [85].

The deployment of smart cities such as Songdo in South Korea [86] and Padova City of Italy [87] are delivering the expected results. Nonetheless, these smart cities are costly to build, and that is why, not all countries, regardless of developed or developing, may support it. Note, however, that smart cities do not always come at a high price. Green [88] present more efficient solutions and frameworks of building and sustaining smart cities less expensively.

Due to the wide variety of sensors available, environmental monitoring can be performed efficiently [89]. Tiny smart sensors such as smart dust [90] can monitor the weather forecast and other relevant data that can be used to detect natural disasters earlier as well as plan the vocation and other services for tourists, etc.

Service and Middleware layer: IoT middleware is a core component in the entire IoT paradigm [34]. Ngu et al. [34] discussed the architecture of IoT middleware in three different classes: in class (a) IoT middleware is constructed as service-based; class (b) is actor-based; and class (c) is an actor-based model by the Terra Swam Research Center [91].

According to Fig. 4, the authors [34] engaging in research work on IoT middleware divided the implementation proposal of IoT middleware into three classes. They are: service-based, cloud-based, and actor-based IoT middleware. The service-based middleware originates from the SOA of the IoT five-layer model. Application and services are at the top and middleware services such as access control, storage, web interface, virtual sensor, and QoS, and event processing services are in the middleware. The

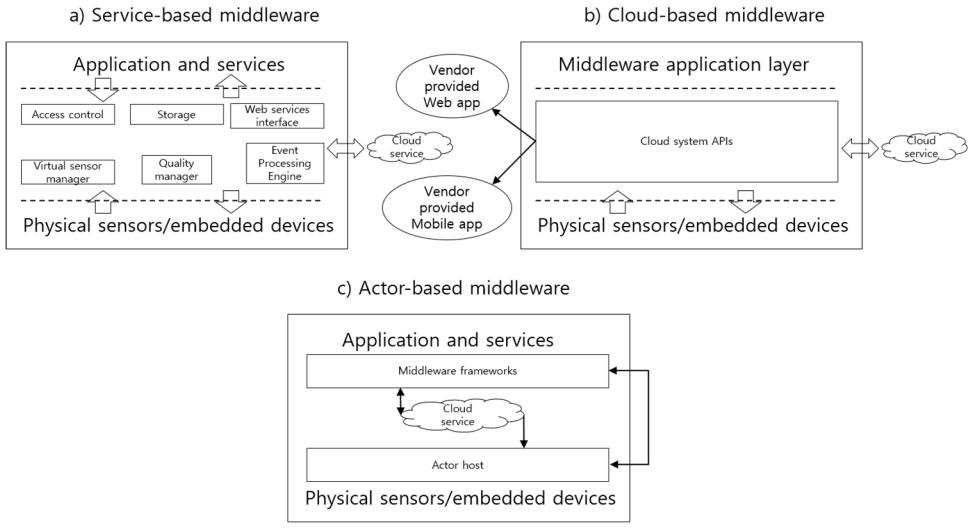

Fig. 4. IoT Middleware frameworks: (a) service-based, (b) cloud-based, and (c) actor-based.

middleware services communicate with cloud services. Below all this architecture lies the actual sensors and actuators as virtual objects. Section (b) below presents a cloud-based model wherein, instead of several middleware services from the Service-based architecture here, lies the cloud system programming interface that supports web and mobile app. On the other hand, actor-based middleware depicts actor, host, and middleware frameworks as sub-middleware layers for the cloud service interaction. These sub-middleware layers also interact with each other.

Fig. 5 shows the entire overview of the IoT middleware discussed above. Due to the need for IoT frameworks, many middleware techniques have been developed, and they are still in progress. GSN, Hydra, Paraimpu, Xively, GoogleFit, Ptolomey's Swarmlet, Node-RED, and Calvin are among them.

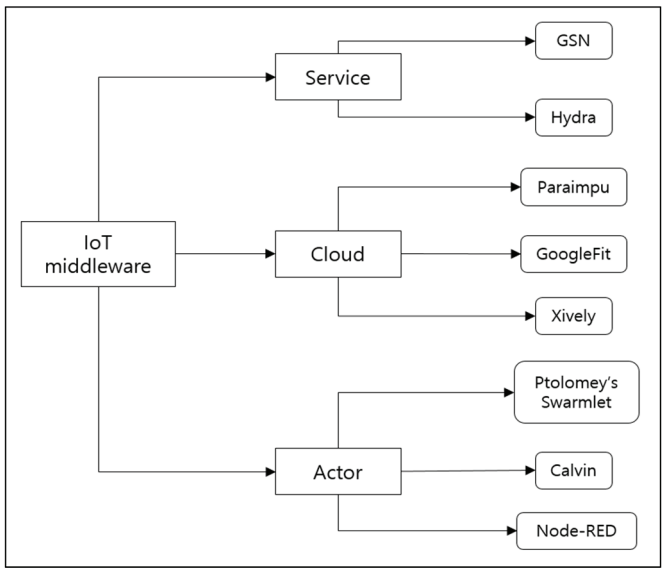

Fig. 5. IoT Middleware overview.

Edge computing: Due to massive data input and output to cloud servers and bottleneck [22] problems, an additional computation layer is established. This layer carries the name fog/edge computing [21,22,32]. Edge computing works solely through standard network protocols as well as with the combination of cellular networks such as 4G and 5G. MEC and MCC are terms used for the collaboration of mobile network and edge/cloud computing servers. In some materials, edge computing can also be referred as gateway to cloud servers [32].

Edge computing forms two methods of implementations: hierarchical and software-defined network-based [21]. The early hierarchical model proposed [92] depicted the integration of MEC into cloudlet infrastructure. Compared to cloud infrastructure, users can request processing of needs, and storage and computing power will be provided in the edge layer. In the software-defined model, however, the costs of management and administration are significantly reduced [92]. The edge operating system [93 is implemented with various open source technologies providing powerful network and service platform, including the [94] proposed integration of SDN, MEC, and network function virtualization (NFV) as well as [95] software-defined infrastructure on the smart edge architecture.

Edge computing architecture consists of three layers [21] (Fig. 6). In this form, users will get some benefits because Edge computing supports fast response and high computational capacity. Note, however, that edge computing has a limitation, i.e., the server cannot provide massive storage unlike cloud servers. Meanwhile, edge computing allows edge nodes to be distributed, and it is dynamic [21]. Due to the increase in the number of edge nodes in the physical environment, edge servers will mostly be available to handle request operations for a convenient user experience.

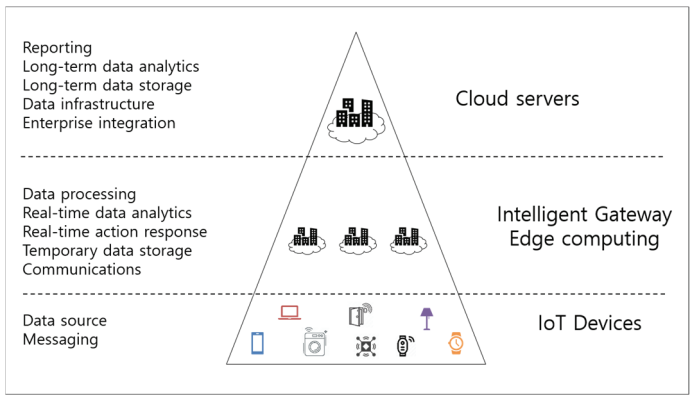

Fig. 6. Edge computing architecture.

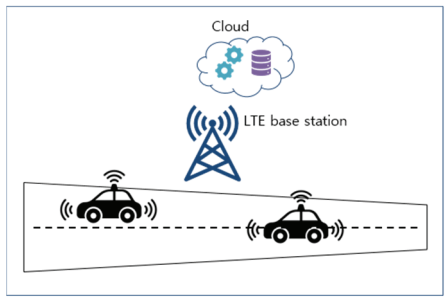

Fig. 7. Vehicular edge paradigm.

Edge computing can also support smart transportation with the combination of the existing cellular network of GSM and 5G. Thus, self-driving cars can receive up-to-date information such as traffic congestion [32] and work autonomously (Fig. 7).

Connectivity: Just as important as the network layer is the connections layer, one of the vital layers in IoT because it provides data transmission services. Due to limited energy and basic computational power of embedded systems, several new protocols have been established as described in the following sections.

- **6LoWPAN:** Low-power wireless personal area network [96]. This protocol provides numerous benefits including small packet size, low power, and low bandwidth, and packets can also be tunneled over IEEE 802.15.4 [97]. Moreover, 6LoWPAN is compatible with older technologies, and it offers better connectivity. It consumes low energy and supports ad-hoc self-organizations. Due to these benefits, it is a perfect option for IoT connectivity.

- **Message Queue Telemetry Transport (MQTT):** Lightweight, it publishes/subscribes to messaging protocol. Data collected from sensors will be directed to servers [30] in a publish/subscribe manner. This protocol supports low bandwidth and high latency. MQTT is a good option to use between sensors, actuators, and servers (Fig. 8).

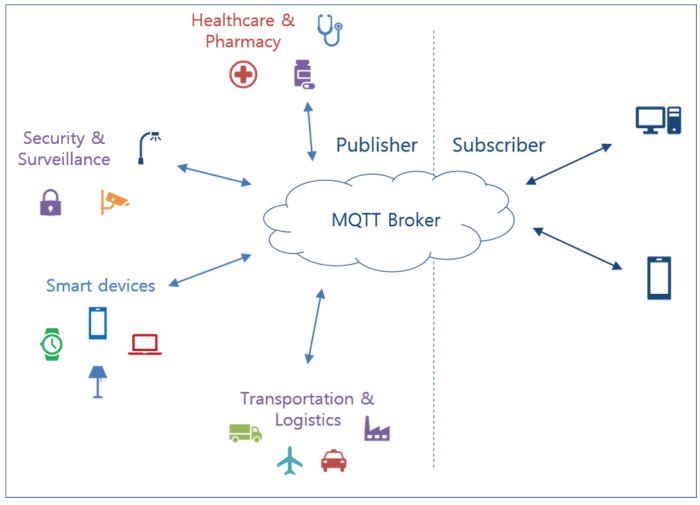

Fig. 8. MQTT protocol mechanism.

- **ZigBee:** As a wireless network protocol, ZigBee works in several layers [96], and it was built for short-term communication with low energy consumption [98]. Economically, ZigBee incurs low cost to acquire, consumes less energy, has reliability, and provides a comprehensive security mechanism as well as supports several topologies including star, mesh, and tree [99].

- **Z-Wave:** This protocol is suitable for low bandwidth network. Note, however, that Z-Wave supports up to 232 nodes, and all nodes can route to each other at the same time [96]. In addition, Z-Wave supports dynamic routing wherein each node can store a routing list separately with updates by controller [68]. Z-Wave consumes less energy and supports reliable transmission [98].

- **IEEE 802.15.4:** The protocol is based on the OSI model, with lower layers providing services to the upper layers and every layer performing partial implementation. Bandwidth of 868/915 M and 2.4 GHz are supported. Transmission reaches up to 250 Kb/s [30]. This protocol is the foundation of other

lightweight protocols such as ZigBee, WirelessHART and others. The main benefits are low energy consumption, low cost, and transmission at low rate [48].

Standardization efforts for IoT together with IoT-layered architecture enhancements are also maturing. IETF standardization [100] establishes the cooperation and integration of protocols and hardware technologies as gateway, too. Table 3 lists the existing IoT protocols such as CoAP, MQTT, XMPP, DDS, RPL, 6LoWPAN, ZigBee, Z-Wave, IEEE 1905.1, etc.

Table 3. IoT protocols

	Protocols					
Application	CoAP	MQTT	XMPP	DDS	AMQP	HTTP REST
Service	mDNS	mDNS	mDNS	DNS-DS	DNS-DS	DNS-DS
Middleware layer						
Routing	RPL	RPL	RPL	RPL	RPL	RPL
Network	6LoWPAN	6LoWPAN	6LoWPAN	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6
Data link	Z-Wave	ZigBee	EPCglobal	EPCglobal	IEEE 802.15.4	LTE-A
Edge node	IEEE 1888.3, IPSec	IEEE 1888.3, IPSec	IEEE 1888.3, IPSec	IEEE 1888.3, IPSec	IEEE 1905.1	IEEE 1905.1

- **Constrained Application Protocol (CoAP):** CoAP is an application layer protocol (Fig. 9). Due to the complexity in HTTP and inappropriateness to use with IoT, CoAP was designed to be a replacement. Group and push communication excluding broadcasting are supported by CoAP, which provides the following key features: reliable security, interaction with HTTP, resource observation, discovery, and block-wise resource transport [30]. CoAP was built upon REST architecture [66].

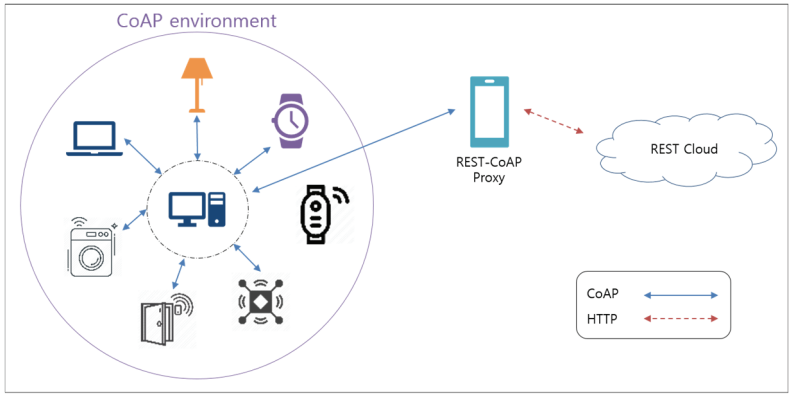

Fig. 9. CoAP Protocol model.

- **Extensible Messaging and Presence Protocol (XMPP):** Based on XML [30], it supports scalability and addressing and provides reliable security. It enables duplex transmission so it is suitable for chatting, voice, and video streaming applications that might be suitable for Smart Home Applications. XMPP has the following three roles, client, server, and gateway – and it can work with TCP/IP Protocol Suite (Fig. 10).

- **Data Distribution Service (DDS):** Like MQTT, DDS is a publish/subscribe protocol [30]. DDS is data-centric protocol that allows supporting excessive QoS, scalability, and reliable communication [67]. Broker-less architecture makes it more suitable for resource-constrained IoT devices.

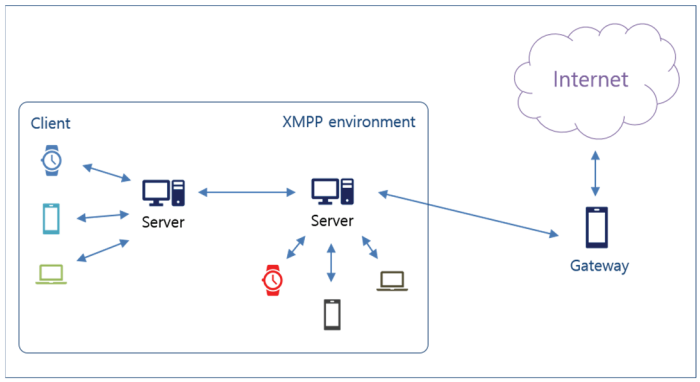

Fig. 10. XMPP protocol architecture.

- **Advanced Message Queueing Protocol (AMQP):** As an open standard protocol, AMQP was designed for message service in the application layer such as queuing and routing (Fig. 11). It supports multiple programming languages and provides stable communication. AMQP uses numerous types of architectures [65] from publish/subscribe mechanism to other mechanisms such as store and forward, message distribution, message queuing, context-based routing, point-to-point routing, and message exchange.

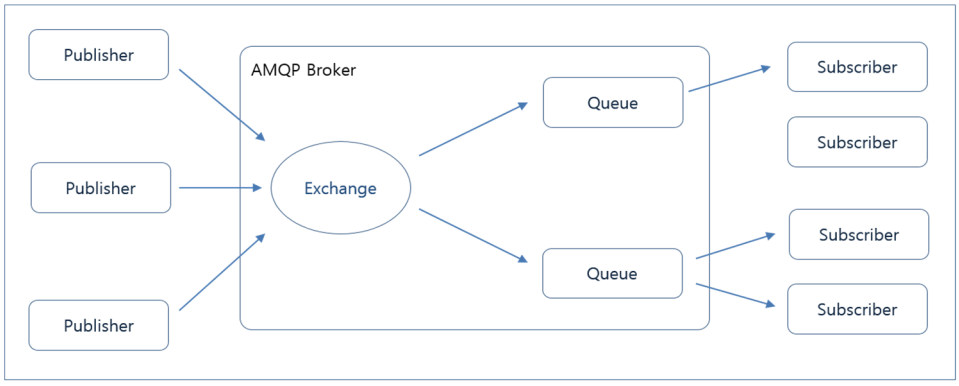

Fig. 11. AMQP protocol architecture.

- **Edge nodes:** Internet of Things has a wide variety of architectural components [2,5]. Since the name from IoT implies "things," however, the foundation for IoT will be the actual sensors and actuators, and the recent development of many wireless smart devices will benefit the entire IoT ecosystem [3,8, 10].

The building blocks of IoT are always things. Fig 12 shows the basic structure of the IoT model. Of course, the specific application paradigm architecture of IoT may vary on a case by case basis [8,10]. Again, however, IoT is composed of things, and by things we refer firstly to sensors and actuators, including RFID tags and readers [33]. Embedded systems that perform a small amount of processing, which provides data transmission through the Internet, are also a thing [36]. Even smart devices including smart watches, smart phones and tablets, laptops, surveillance technologies, and smart driverless cars are part of IoTs. Basic services such as route and train tracking already exist in various developed countries, and South Korea's metro system [101 benefits a lot of citizens.

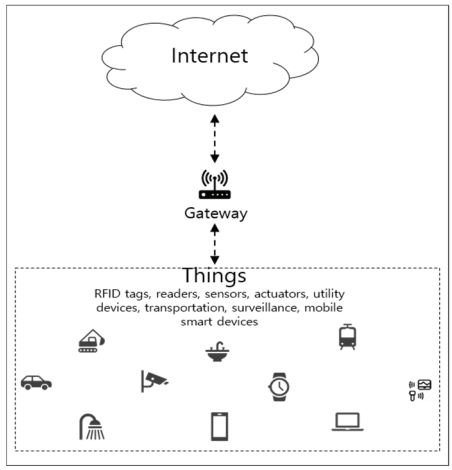

Fig. 12. IoT "things".

Additional components for IoT are also worth mentioning, such as Mobile Edge/Cloud Computing, Cyber Physical Systems [44], and Edge Computing [21]. Internet of Things already covers a wide area of research topics as it includes all fields in computing from software engineering to machine learning as a sublayer of artificial intelligence [102].

Economic perspectives: Internet of Things is referred to as the fourth industrial revolution [75]; consequently, it is interesting to know about the IoT market share. IoT will serve various types of industries from smart homes such as consumer market to healthcare, vehicles, agriculture, smart city infrastructure, retail market, manufacturing, and security services [30].

Based on the data in Fig. 13, the largest market share belongs to the healthcare and manufacturing industries. The healthcare industry is supported by various medical sensors as well as patient monitoring and other numerous services [30]. On the other hand, manufacturing is an integration of cyber physical systems as well as robotics, computer vision [30], and other related sensor and actuator technologies.

Accounting for the remaining market shares are household utilities control services [103], resource extraction services, smart car and autonomous driving [104], smart city infrastructure [24,35,69], agriculture sectors [16,17] and e-commerce [18].

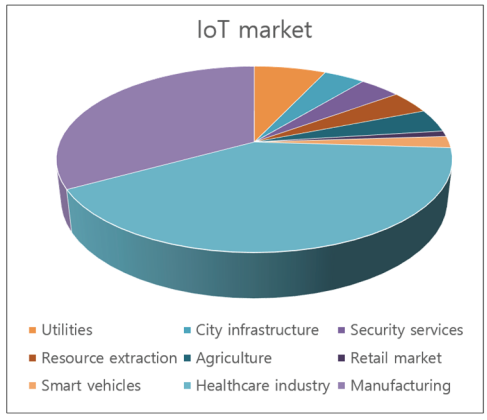

Fig. 13. IoT market size.

4. IoT Security

Security requirements: The authors [2,4] proposed a combination of eight security requirements from CIA-triad and IAS-octave. Table 4 presents the eight different security requirements. Confidentiality involves allowing access to authorized users only, whereas Integrity means the absence of unauthorized data modification. Availability is providing users with existing services anytime upon request, etc. Abbreviations are provided for all security requirements.

These requirements are very important that each stand for one functionality in the system, and security threats discussed in later sections can break one or many of these requirements. For instance, in the healthcare industry, patient privacy is an important aspect, and unauthorized access to data may lead to breaking the Integrity requirement, even causing the invasion of patients' privacy and life-threatening incidents [71].

Table 4. Requirements for IoT security

Name	Description	Abbreviation
Confidentiality	Access to authorized users only	C
Integrity	Absence of unauthorized data modification by ensuring completeness and accuracy	I
Availability	Making services available upon request	A
Accountability	Being accountable for the actions of the users	AC
Auditability	Control of actions persistently	AU
Trustworthiness	Verifying identity and establishing trust for third party	TW
Non-repudiation	System has confirmation for the occurrence or non-occurrence of an action	NR
Privacy	Implementing robust privacy policies and letting users control their own information	P

Security threats for IoT: Starting from the recent exploitations on IoT devices from DDoS attack [70], state-of-the-art research is also ongoing [64,105,106] on defending IoT devices from threat and sustaining user privacy and following common policies as well as other security risks in IoT including, hardware Trojans, side-channel attacks, physical and routing attack, etc. [4,107] (Fig. 14)

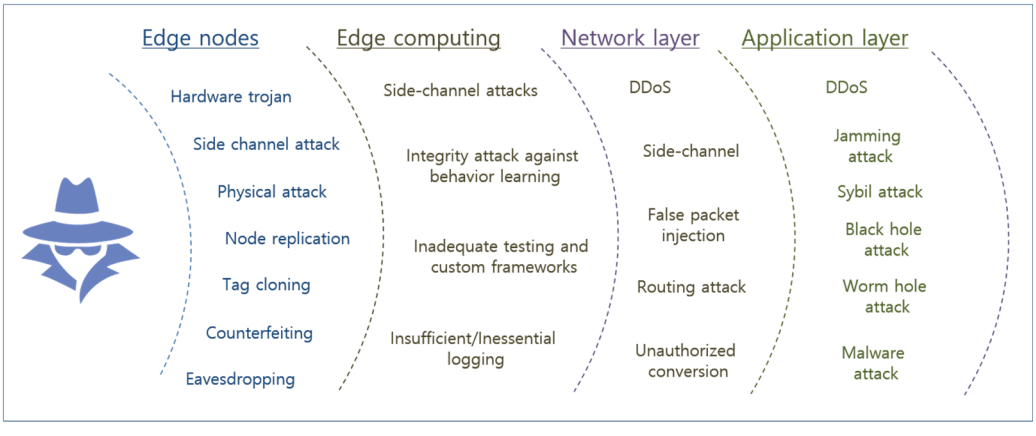

Fig. 14. IoT security threats.

Numerous security threats exist on each layer of IoT. Earlier, we mentioned that the last comprehensive IoT architecture is the seven-layer CISCO reference model [12]. In this survey, however, we selected the four main layers of IoT and security threats that may cause damage [4,107]. We propose the following countermeasures for the security risks:

Hardware Trojans: The modification of the integrated circuit causes hardware Trojans to occur. The attacker may maliciously change the design of the circuit board and call the mechanism remotely or within the device with a special trigger. Various side channel signals using timing, power and spatial temperature [108], and Trojan activation techniques [108] can be used for Trojan detection.

Side-channel attack: A device operating normally without being intruded upon or exploited may reveal some valuable information in case of information leak. The electromagnetic (EM) signature from a few sensors and actuators may reveal the status of the device [72], so an intruder can acknowledge and perform some actions on it. Side-channel signal analysis is a method for detecting and preventing malicious firmware and software.

Denial of Service (DoS) attacks: This is a form of attack wherein legitimate users are blocked from the services of the system. Battery draining on sensors and actuators, Sleep deprivation, and outage attacks are possible cases of DoS in IoT. Trojan activation can be used to detect hardware Trojans [4]. Dao et al. [64] propose the behavior learning of a DDoS attack by applying smart filters composed of SOM.

Physical attacks: IoT devices are usually left in open environments such as public places, hospitals, etc. due to lack of harm to the public. For these reasons, however, they are vulnerable to physical damage or tampering attacks by intruders [4]. On the other hand, physical attacks may cause permanent damage. As an example [109], Nest thermostat was attacked by physical intrusion with the intention of replacing the firmware, which may give permission to the malicious user to control and access it remotely.

Node replication attack: By replicating the existing nodes in the network, the malicious user adds a node that mimics one of the existing nodes. This attack is launched to obtain valuable information from the system and cause permanent damage [110]. Cryptographic schemes such as encryption and hash-based schemes are used to prevent security risks on IoT edge nodes [4]. Due to computational limitations, lightweight cryptographic mechanism is supported as well [111].

Tag cloning: With alternative name spoofing, as the name implies, similar to node replication, the method involves creating a clone from the existing nodes and using it for malicious purposes [4]. Kill Sleep command and blocking and distance estimation [73] methods can be applied to prevent this attack [4].

Counterfeiting: Partial manipulation of the tag or IoT device is performed to use the node for malicious purposes or cause damage [4]. A personal firewall dedicated to constrained devices can be used to prevent this type of threat [74].

Eavesdropping: A malicious user intercepts, reads, and stores a copy of messages for later use. Copied data can be used for other forms of attack such as tag cloning [4]. Eavesdropping like DDoS attacks is a critical concern for IoT. Personal firewalls and cryptographic schemes are applied to prevent the threat [4,110].

Inadequate testing and custom framework: Standardization is the best method of providing quality of services and preventing security risks. Due to ease of building and sale opportunities and growing demand from the market, however, more startups and small companies join the IoT business, and inadequate standardization may occur [110]. For this reason, some security holes may be found [4]. To

prevent such occasion, a pre-testing method is required [73].

Insufficient logging: Insufficient logging can cause damage to the system and reveal no spots for intrusion details [4]. Encrypted comprehensive logging is the best method of detecting hacking attacks and avoiding any intrusions [4].

False packet injection: Through insertion, manipulation, and replication, attackers can inject false packets into network links [4]. Protocol header update, checksum, and packet manipulation can be done by capturing the legitimate user data [4]. Intrusion Detection Systems dedicated to embedded systems can be applied to prevent such threats [73].

Routing attack: This involves preventing the proper communication of devices. Routing attacks may have several other forms: *Black hole attack,* which attracts the network by proposing a shortcut route and, through this call, captures the data while sending packets to the destination; *Worm hole attack* occurs even without breaking authentication rules, wherein an attacker records packets in one location and tunnels them in another place; and *Sybil attack* is a threat wherein an attacker constructs a fake identity and replicates the actual node in the network. In a routing attack, a malicious user modifies the routing information of the packets so that the data may be directed to the malicious user, dropped on the route, or misdirected [4]. Reliable routing methods such as application of lightweight cryptography protocols or sending of data through secure channels or frameworks are applied to prevent routing attacks [4].

Unauthorized conversion: This type of threat occurs when nodes in the environment share data with every other unintentional node, which can cause the threat of a malicious user accessing the whole IoT environment and remotely controlling it [4].

Malware attack: Malicious software such as virus, worms, and ransomware [107] solely affects the operating system but can cause severe damage to applications. For example, injecting worms in smart city infrastructure can cause privacy issues in administration, businesses, and residents alike. Adaptation and commercialization of anti-malware and anti-virus software for IoT are future trends [107].

5. Conclusion and Future Topics

In this comprehensive survey, we tried to cover information on IoT technologies, applications, and security aspects. We discussed the related survey and research works to date and explored the status and IoT development life cycle. We also approached the various applications of IoT and its security aspects. We believe the information we provided and references we collected will benefit other researchers.

Based on the survey outcomes above, we believe that edge computing and machine learning applications to threat detection and analysis, design and implementation, and perspective research on MEC/MCC and anti-virus and anti-malware software for IoTs can be future topics.

Acknowledgement

This work was supported by Institute for Information communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No. B0184-15-1003, oneM2M The Development of oneM2M Conformance Testing Tool and QoS Technology).

References

[1] F. Mattern and C. Florkemeier, "Vom internet der computer zum internet der dinge," *Informatik-Spektrum*, vol. 33, no. 2, pp. 107-121, 2010.

[2] 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 of Things Journal*, vol. 4, no. 5, pp. 1125-1142, 2017.

[3] K. K. Patel and S. M. Patel, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," *International Journal of Engineering Science and Computing*, vol. 6, no. 5, pp. 6122-6131, 2016.

[4] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586-602, 2016.

[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, 2010.

[6] R. Buyya and A. Dastjerdi, *Internet of Things Principles and Paradigms.* Cambridge, MA: Morgan Kaufmann, 2016.

[7] A. B. Pawar and S. Ghumbre, "A survey on IoT applications, security challenges and counter measures," in *Proceedings of 2016 International Conference on Computing, Analytics and Security Trends (CAST)*, Pune, India, 2016, pp. 294-299.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): a vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, 2013.

[9] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelffle, *Vision and Challenges for Realising the Internet of Things*. Brussel, Belgium: Cluster of European Research Projects on the Internet of Things, 2010.

[10] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: the internet of things architecture, possible applications and key challenges," in *Proceedings of 2012 10th International Conference on Frontiers of Information Technology*, Islamabad, India, 2012, pp. 257-260.

[11] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497-1516, 2012.

[12] CISCO, "The Internet of Things reference model," 2014 [Online]. Available: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf.

[13] S. U. Maheswari, N. S. Usha, E. M. Anita, and K. R. Devi, "A novel robust routing protocol RAEED to avoid DoS attacks in WSN," in *Proceedings of 2016 International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, India, 2016, pp. 1-5.

[14] F. Palermo, "Internet of Things done wrong stifles innovation," 2014 [Online]. Available: https://www.informationweek.com/strategic-cio/executive-insights-and-innovation/internet-of-things-done-wrong-stifles-innovation/a/d-id/1279157.

[15] A. Singh, S. Meshram, T. Gujar, and P. R. Wankhede, "Baggage tracing and handling system using RFID and IoT for airports," in *Proceedings of 2016 International Conference on Computing, Analytics and Security Trends (CAST)*, Pune, India, 2016, pp. 466-470.

[16] K. A. Patil and N. R. Kale, "A model for smart agriculture using IoT," in *Proceedings of 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC)*, Jalgaon, India, 2016, pp. 543-545.

[17] J. C. Zhao, J. F. Zhang, Y. Feng, and J. X. Guo, "The study and application of the IOT technology in agriculture," in *Proceedings of 2010 3rd International Conference on Computer Science and Information Technology*, Chengdu, China, 2010, pp. 462-465.

[18] Z. Ju and Y. Li, "Analysis on Internet of Things (IOT) based on the "Subway Supermarket" e-commerce mode of TESCO," in *Proceedings of 2011 International Conference on Information Management, Innovation Management and Industrial Engineering*, Shenzhen, China, 2011, pp. 430-433.

[19] F. J. Wu, Y. F. Kao, and Y. C. Tseng, "From wireless sensor networks towards cyber physical systems," *Pervasive and Mobile Computing*, vol. 7, no. 4, pp. 397-413, 2011.

[20] A. R. Biswas and R. Giaffreda, "IoT and cloud convergence: opportunities and challenges," in *Proceedings of 2014 IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, Korea, 2014, pp. 375-376.

[21] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900-6919, 2017.

[22] T. Subramanya, L. Goratti, S. N. Khan, E. Kafetzakis, I. Giannoulakis, and R. Riggio, "A practical architecture for mobile edge computing," in *Proceedings of 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, Berlin, Germany, 2017, pp. 1-4.

[23] S. Mumtaz, K. M. S. Huq, and J. Rodriguez, "Direct mobile-to-mobile communication: paradigm for 5G," *IEEE Wireless Communications*, vol. 21, no. 5, pp. 14-23, 2014.

[24] P. Yadav and S. Vishwakarma, "Application of Internet of Things and big data towards a smart city," in *Proceedings of 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Bhimtal, India, 2018, pp. 1-5.

[25] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for Internet of Things data analysis: a survey," *Digital Communications and Networks*, vol. 4, no. 3, pp. 161-175, 2018.

[26] M. Weiser, "The computer for the 21st century," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 3, no. 3, pp. 3-11, 1999.

[27] N. Gyory and M. Chuah, "IoTOne: integrated platform for heterogeneous IoT devices," in *Proceedings of 2017 International Conference on Computing, Networking and Communications (ICNC)*, Santa Clara, CA, 2017, pp. 783-787.

[28] P. Gaur and M. P. Tahiliani, "Operating systems for IoT devices: a critical survey," in *Proceedings of 2015 IEEE Region 10 Symposium*, Ahmedabad, India, 2015, pp. 33-36.

[29] K. Xu, Y. Qu, and K. Yang, "A tutorial on the internet of things: from a heterogeneous network integration perspective," *IEEE Network*, vol. 30, no. 2, pp. 102-108, 2016.

[30] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.

[31] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): a literature review," *Journal of Computer and Communications*, vol. 3, pp. 164-173, 2015.

[32] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: a survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450-465, 2018.

[33] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure Internet of Things," in *Proceedings of 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, Vienna, Austria, 2016, pp. 84-90.

[34] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT middleware: a survey on issues and enabling technologies," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 1-20, 2016.

[35] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22-32, 2014.

[36] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, and W. Zhao, "How can heterogeneous Internet of Things build our future: a survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2011-2027, 2018.

[37] N. Aleisa and K. Renaud, "Privacy of the Internet of Things: a systematic literature review (extended discussion)," 2016 [Online]. Available: https://arxiv.org/abs/1611.03340.

[38] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats to Internet-of-Things (IoT) devices and applications," 2018 [Online]. Available: https://arxiv.org/abs/1802.02041.

[39] S. Bera, S. Misra, and A. V. Vasilakos, "Software-defined networking for internet of things: a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1994-2008, 2017.

[40] S. H. Ahmed, G. Kim, and D. Kim, "Cyber physical system: architecture, applications and research challenges," in *Proceedings of 2013 IFIP Wireless Days (WD)*, Valencia, Spain, 2013, pp. 1-5.

[41] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: security vulnerabilities and challenges," in *Proceedings of 2015 IEEE Symposium on Computers and Communication (ISCC)*, 2015, pp. 180-187.

[42] M. V. Bharathi, R. C. Tanguturi, C. Jayakumar, and K. Selvamani, "Node capture attack in wireless sensor network: a survey," in *Proceedings of 2012 IEEE International Conference on Computational Intelligence and Computing Research*, Coimbatore, India, 2012, pp. 1-3.

[43] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, Helsinki, Finland, 2012, pp. 13-16.

[44] A. Botta, W. De Donato, V. Persico, and A. Pescape, "On the integration of cloud computing and Internet of Things," in *Proceedings of 2014 International Conference on Future Internet of Things and Cloud*, Barcelona, Spain, 2014, pp. 23-30.

[45] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: towards survivable cyber-physical systems," in *Proceedings of 2008 the 28th International Conference on Distributed Computing Systems Workshops*, Beijing, China, 2008, pp. 495-500.

[46] Z. Chen, G. Xu, V. Mahalingam, L. Ge, J. Nguyen, W. Yu, and C. Lu, "A cloud computing based network monitoring and threat detection system for critical infrastructures," *Big Data Research*, vol. 3, pp. 10-23, 2016.

[47] X. Fu, Z. Ling, W. Yu, and J. Luo, "Cyber Crime Scene Investigations (C^2SI) through cloud computing," in *Proceedings of 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops*, Genova, Italy, 2010, pp. 26-31.

[48] G. Gan, Z. Lu, and J. Jiang, "Internet of Things security analysis," in *Proceedings of 2011 International Conference on Internet Technology and Applications*, Wuhan, China, 2011, pp. 1-4.

[49] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in *Proceedings of 2014 Euro Med Telco Conference (EMTC)*, Naples, Italy, 2014, pp. 1-5.

[50] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: current status, challenges and prospective measures," in *Proceedings of 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, UK, 2015, pp. 336-341.

[51] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, Berkeley, CA, 2004, pp. 259-268.

[52] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud computing: security issues and research challenges," *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, vol. 1, no. 2, pp. 136-146, 2011.

[53] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637-646, 2016.

[54] V. Soni, P. Modi, and V. Chaudhri, "Detecting Sinkhole attack in wireless sensor network," *International Journal of Application or Innovation in Engineering & Management*, vol. 2, no. 2, pp. 29-32, 2013.

[55] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Proceedings of 2014 Federated Conference on Computer Science and Information Systems*, Warsaw, Poland, 2014, pp. 1-8.

[56] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: a review," in *Proceedings of 2012 International Conference on Computer Science and Electronics Engineering*, Hangzhou, China, 2012, pp. 648-651.

[57] J. Wu and W. Zhao, "Design and realization of WInternet: from net of things to Internet of Things," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 1, article no. 2, 2017.

[58] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, "Research on the architecture of Internet of Things," in *Proceedings of 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, Chengdu, China, 2010, pp. 484-487.

[59] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372-383, 2014.

[60] K. Zhao and L. Ge, "A survey on the internet of things security," in *Proceedings of 2013 9th International Conference on Computational Intelligence and Security*, Leshan, China, 2013, pp. 663-667.

[61] A. M. Nia, M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Energy-efficient long-term continuous personal health monitoring," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 85-98, 2015.

[62] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system," in *Proceedings of 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*, Columbia, MO, 2011, pp. 150-156.

[63] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses," in *Proceedings of 2008 IEEE Symposium on Security and Privacy*, Oakland, CA, 2008, pp. 129-142.

[64] N. N. Dao, T. V. Phan, J. Kim, T. Bauschert, and S. Cho, "Securing heterogeneous IoT with intelligent DDoS attack behavior learning," 2017 [Online]. Available: https://arxiv.org/abs/1711.06041.

[65] S. Schneider, "Understanding the protocols behind the Internet of Things," 2013 [Online]. Available: https://www.electronicdesign.com/iot/understanding-protocols-behind-internet-things.

[66] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: an application protocol for billions of tiny internet nodes," *IEEE Internet Computing*, vol. 16, pp. 62-67, 2012.

[67] Object Management Group, "Data Distribution Service (DDS), version 1.2," 2007 [Online]. Available: https://www.omg.org/spec/DDS/1.2/About-DDS/.

[68] C. Gomez and J. Paradells, "Wireless home automation networks: a survey of architectures and technologies," *IEEE Communications Magazine*, vol. 48, no. 6, pp. 92-101, 2010.

[69] Y. Liu, "The study on smart city construction assessment based on TOPSIS—"the Beijing-Tianjin-Tangshan City Clusters" as the case," in *Proceedings of 2016 International Conference on Smart City and Systems Engineering (ICSCSE)*, Hunan, China, 2016, pp. 321-325.

[70] S. Weagle, "The rise of IoT botnet threats and DDoS attacks," 2018. [Online]. Available: https://www.corero.com/blog/870-the-rise-of-iot-botnet-threats-and-ddos-attacks.html.

[71] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1174-1188, 2014.

[72] A. M. Nia, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Physiological information leakage: a new frontier in health information security," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 3, pp. 321-334, 2016.

[73] A. Juels, "RFID security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-394, 2006.

[74] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "RFID Guardian: a battery-powered mobile device for RFID privacy management," in *Information Security and Privacy*. Heidelberg: Springer, 2015, pp. 184-194.

[75] F. Griffiths and M. Ooi, "The fourth industrial revolution-Industry 4.0 and IoT [Trends in Future I&M]," *IEEE Instrumentation & Measurement Magazine*, vol. 21, no. 6, pp. 29-43, 2018.

[76] G. Press, "A very short history of Internet of Things," 2014 [Online]. Available: https://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/.

[77] Wikipeia, "Internet of Things," [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_things#cite_noteETC:_Bill_Joy's_Six_Webs-12.

[78] Postscapes, "Internet of Things (IoT) history," [Online]. Available: https://www.postscapes.com/internet-of-things-history/.

[79] J. Porter, "The history of Internet of Things (IoT) and how it's changed today," 2018 [Online]. Available: https://www.techprevue.com/history-iot-changed-today/.

[80] W. Belk, "Visual history of IoT – far beyond 'smart' things," 2016 [Online]. Available: https://medium.com/@wbelk/visual-history-of-iot-far-beyond-smart-things-325664d9794.

[81] J. Van Camp, "The 8 best smart speakers with Alexa and Google Assistant," 2019 [Online]. Available: https://www.wired.com/story/best-smart-speakers/.

[82] M. Cho, "Kakao AI speaker begins official sales," 2017 [Online]. Available: https://www.zdnet.com/article/kakao-ai-speaker-begins-official-sales/.

[83] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A survey on facilities for experimental internet of things research," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 58-67, 2011.

[84] P. Brizzi, D. Conzon, H. Khaleel, R. Tomasi, C. Pastrone, A. M. Spirito, M. Knechtel, F. Pramudianto, and P. Cultrona, "Bringing the Internet of Things along the manufacturing line: a case study in controlling industrial robot and monitoring energy consumption remotely," in *Proceedings of 2013 IEEE 18th Conference on Emerging Technologies & Factory Automation (ETFA)*, Cagliari, Italy, 2013, pp. 1-8.

[85] M. S. Rahman, A. H. M. Noman, F. Shahari, M. Aslam, C. S. Gee, C. R. Isa, and S. Pervin, "Efficient energy consumption in industrial sectors and its effect on environment: a comparative analysis between G8 and Southeast Asian emerging economies," *Energy*, vol. 97, pp. 82-89, 2016.

[86]] S. Richardson, "Welcome to Songdo, South Korea: the smartest of smart cities," 2018 [Online]. Available: https://www.worldcrunch.com/smarter-cities-1/welcome-to-songdo-south-korea-the-smartest-of-smart-cities.

[87] A. Cenedese, A. Zanella, L. Vangelista, and M. Zorzi, "Padova smart city: an urban internet of things experimentation," in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, Sydney, Australia, 2014, pp. 1-6.

[88] J. Green, "Green cities on the cheap: low-cost solutions for a sustainable world," 2011 [Online]. Available: https://grist.org/smart-cities/2011-12-28-green-cities-on-the-cheap-low-cost-solutions-sustainable-world/.

[89] M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 45-54, 2013.

[90] M. Sharifi, S. S. Kashi, and S. P. Ardakani, "Lap: a lightweight authentication protocol for smart dust wireless sensor networks," in *Proceedings of 2009 International Symposium on Collaborative Technologies and Systems*, Baltimore, MD, 2009, pp. 258-265.

[91] The TerraSwarm Research Center [Online]. Available: https://terraswarm.org.

[92] Y. Jararweh, A. Doulat, O. AlQudah, E. Ahmed, M. Al-Ayyoub, and E. Benkhelifa, "The future of mobile cloud computing: integrating cloudlets and mobile edge computing," in *Proceedings of 2016 23rd International Conference on Telecommunications (ICT)*, Thessaloniki, Greece, 2016, pp. 1-5.

[93] A. Manzalini and N. Crespi, "An edge operating system enabling anything-as-a-service," *IEEE Communications Magazine*, vol. 54, no. 3, pp. 62-67, 2016.

[94] O. Salman, I. Elhajj, A. Kayssi, and A. Chehab, "Edge computing enabling the Internet of Things," in *Proceedings of 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Italy, 2015, pp. 603-608.

[95] T. Lin, B. Park, H. Bannazadeh, and A. Leon-Garcia, "Demo abstract: End-to-end orchestration across SDI smart edges," in *Proceedings of 2016 IEEE/ACM Symposium on Edge Computing (SEC)*, Washington, DC, 2016, pp. 127-128.

[96] J. Tan and S. G. Koo, "A survey of technologies in Internet of Things," in *Proceedings of 2014 IEEE International Conference on Distributed Computing in Sensor Systems*, Marina Del Rey, CA, 2014, pp. 269-274.

[97] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (important) things," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1389-1406, 2012.

[98] H. B. Pandya and T. A. Champaneria, "Notice of retraction Internet of Things: survey and case studies," in *Proceedings of 2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO)*, Visakhapatnam, India, 2015, pp. 1-6.

[99] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: a survey on the state of the art and the 802.15. 4 and ZigBee standards," *Computer Communications*, vol. 30, no. 7, pp. 1655-1695, 2017.

[100] I. Ishaq, D. Carels, G. K. Teklemariam, J. Hoebeke, F. van den Abeele, E. De Poorter, I. Moerman, and P. Demeester, "IETF standardization in the field of the Internet of Things (IoT): a survey," *Journal of Sensor and Actuator Networks*, vo. 2, no. 2, pp. 235-287, 2013.

[101] Y. Lee, "How to navigate your way through Seoul," 2018 [Online]. Available: https://10mag.com/how-to-navigate-your-way-through-seoul/.

[102] J. S. Jang, Y. L. Kim, and J. H. Park, "A study on the optimization of the uplink period using machine learning in the future IoT network," in *Proceedings of 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, Sydney, Australia, 2016, pp. 1-3.

[103] M. Suresh, U. Muthukumar, and J. Chandapillai, "A novel smart water-meter based on IoT and smartphone app for city distribution management," in *Proceedings of 2017 IEEE Region 10 Symposium (TENSYMP)*, Cochin, India, 2017, pp. 1-5.

[104] G. A. Babu, K. Guruvayoorappan, V. S. Variyar, and K. P. Soman, "Design and fabrication of robotic systems: converting a conventional car to a driverless car," in *Proceedings of 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Udupi, India, 2017, pp. 857-863.

[105]] D. Anstee, P. Bowen, C. F. Chui, and G. Sockrider, "Worldwide Infrastructure Security Report (volume XII)," Arbort Networks special report, 2017.

[106] E. Leverett and A. Kaplan, "Towards estimating the untapped potential: a global malicious DDoS mean capacity estimate," *Journal of Cyber Policy*, vol. 2, no. 2, pp. 195-208, 2017.

[107] A. Alsaidi and F. Kausar, "Security attacks and countermeasures on cloud assisted IoT applications," in *Proceedings of 2018 IEEE International Conference on Smart Cloud (SmartCloud)*, New York, NY, 2018, pp. 213-217.

[108] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10-25, 2010.

[109] G. Hernandez, O. Arias, D. Buentello, and Y. Jin, "Smart nest thermostat: a smart spy in your home," in *Proceedings of the Black Hat*, Las Vegas, NV, 2014, pp. 1-8.

[110] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: a survey," in *Security in Distributed, Grid, Mobile, and Pervasive Computing*. Boca Raton, FL: CRC Press, 2007, pp. 367-410.

[111] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "M2AP: a minimalist mutual-authentication protocol for low-cost RFID tags," in *Ubiquitous Intelligence and Computing*. Heidelberg: Springer, 2006, pp. 912-923.

Khusanbek Gafurov https://orcid.org/0000-0001-6185-0373

He is pursuing M.S. degree in College of Information and Communication Engineering at Sungkyunkwan University since 2017. The same year, he joined Internet Management Technology Lab as a graduate researcher assistant. His research field is IoT and IoT security.

Tai-Myoung Chung https://orcid.org/0000-0002-3154-1868

He is a professor and dean of College of Software at Sungkyunkwan University since 1995. He received Ph.D. degree from Purdue University and M.S. degree from University of Illinois, respectively. His research interests include computer and network security, software defined networking, Internet and IoT Security.