Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics

Yang Lu, *Member, IEEE*, Li Da Xu, *Fellow, IEEE*

***Abstract*—As an emerging technology, the Internet of Things (IoT) revolutionized the global network comprising of people, smart devices, intelligent objects, information, and data. The development of IoT is still in its infancy and many directly related issues need to be solved. IoT is a unified concept of embedding everything. IoT has a great chance to make the world a higher level of accessibility, integrity, availability, scalability, confidentiality, and interoperability. But, how to protect IoT is a challenging task. System security is the foundation for the development of IoT. This article systematically reviews IoT cybersecurity. The key factors of the paradigm are the protection and integration of heterogeneous smart devices and information communication technologies (ICT). Our review applies to people interested in cybersecurity of IoT, such as the current research of IoT cybersecurity, IoT cybersecurity architecture and taxonomy, key enabling countermeasures and strategies, major applications in industries, research trends and challenges.**

***Index Terms*— Cybersecurity, Enterprise Systems, Industrial Informatics, Internet of Things (IoT), Radio Frequency Identification (RFID), Smart Device, Wireless Sensor Networks (WSNs).**

I. Introduction

As an emerging technology and, really, a revolution, the Internet of Things (IoT) has brought tremendous changes to end users in their daily lives. For individuals, their living, studying, and working are all involved in the IoT network, taking advantage of smart environments (home and city), eHealth, and transportation systems. For businesses or institutions, innovations like advanced automation and industrial manufacturing, knowledge sharing and data management, and smart and self-modifying mechanisms and systems are becoming more and more popular [1].

Due to the rapid development in telecommunication systems, IoT can collaborate with Wireless Sensor Networks (WSNs), Radio Frequency Identification (RFID), things, and networks in any form, at any time, and anywhere. Cybersecurity is the inevitable problem that must be solved in the development of IoT. If the issue is not well managed, hackers will take advantage of the defects and weaknesses of devices or objects and then will distort data or disrupt systems through the global IoT network. IoT attacks and failures may outweigh any of its benefits. In addition, traditional security protocols and mechanisms are not suitable because existing devices are limited in their low levels of scalability, integrity, and interoperability. Therefore, new methodologies and technologies should be developed to meet the security, privacy, and reliability requirements of IoT [2]-[4].

IoT involves so many different things, especially heterogeneous devices. By 2015, IoT connected 4.9 billion things and will connect 25 billion things by 2020 [5]. IoT has great flexibility and scalability, but this huge number also may predict a security disaster. The more devices a person connects, the greater the risk to the individual and to the network, and the higher the cybersecurity risk to the global infrastructure. In 2003, each person had only fewer than 0.08 devices. In 2010, the number increased to 1.84. By 2020, there will be 6.58 devices per person [6]. Devices of all types are developing widely and rapidly across the global IoT network, but these devices are easily attacked and are considered as vulnerable points in the IoT network. Thus, the IoT cybersecurity infrastructure ensures that devices are maintained in a secure environment and that users can use them appropriately. The scale of IoT smart devices is very broad, and includes computers, smart phones, communication interfaces, operating systems, lightweight services, and preloaded applications. Equipped with RFID sensors or actuators, intelligent devices can execute accordingly, make decisions autonomously, and disseminate information to users safely [7], [8].

With the advancement of internet and wireless communication, smart devices and things, and IP protocol and sensor network technologies, more and more network-based objects have been involved in IoT cybersecurity. These advanced technologies also are having a huge impact on new ICT and on Industry 4.0 [9]. Cybersecurity is spread across the IoT network, a global infrastructure of heterogeneous smart devices that integrate sensory, communications, networking,

Yang Lu received his B.S. degree from Jilin University, China, in 2004 and the M.S. degree from the University of Manchester, UK, in 2006. He is currently pursuing his Ph.D. degree in ICT (Information and Communication Technology) in USA. He is a member of IEEE. He has published research papers in refereed journals published by major publishers such as Elsevier, Taylor and Francis, and World Scientific (e-mail: y1lu@odu.edu/ziiyuu@gmail.com).

Li Da Xu (M'86–SM'11-F'16) received B.S. degree in information science and engineering from the University of Science and Technology of China, in 1978, M.S. degree in information science and engineering from the University of Science and Technology of China, in 1981, and Ph.D. degree in systems science and engineering from Portland State University, USA, in 1986 (e-mail: LXu@odu.edu). (Corresponding Author).

He is an IEEE Fellow, academician of the European Academy of Sciences, and academician of the Russian Academy of Engineering (formerly USSR Academy of Engineering). Dr. Xu is a 2016 and 2017 Highly Cited Researcher in the field of engineering named by Clarivate Analytics (formerly Thomson Reuters Intellectual Property & Science).

and information processing technologies [1]. In addition, many other technologies and devices, such as barcodes, smart phones, social networks, and cloud computing, that are used in IoT influence cybersecurity, to some extent.

The cybersecurity of IoT is often cited by countries and institutions to implement standards and laws in order to achieve a high degree of cybersecurity. The United States, China, and the United Kingdom are the three largest countries affected by IoT cybersecurity threats, especially by smart home attacks [10]. In the U.S., the Cybersecurity for the Internet of Things (IoT) program has been implemented to control and to improve the cybersecurity of smart devices and the entire environments by standards and guidelines [11]. China's Cybersecurity Law (CSL) was initiated on June 1, 2017. The Cyberspace Administration of China (CAC) is the primary governmental authority to supervise and enforce the CSL. The CSL regulates cybersecurity from different aspects, including network operation security and network information security, as well as managing monitoring, early warning, and emergency responses within mainland China [12]. Europe has made progress in various sectors, such as energy, vehicles, and residential, in cybersecurity [13].

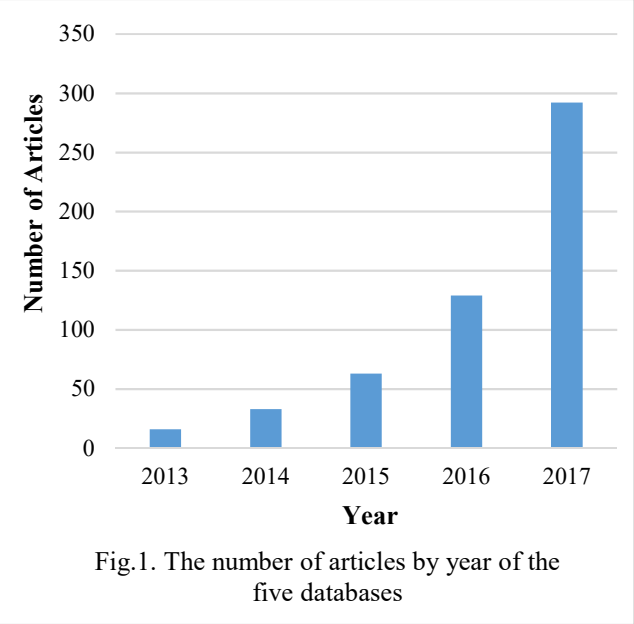

Fig.1. The number of articles by year of the five databases

Despite, or perhaps even because of, the diversified benefits of internets, without powerful cybersecurity infrastructure and functions, security attacks and deliberate misconduct can cause great trouble for the global IoT network. Meanwhile, the number of IoT-related cybersecurity publications is growing exponentially. This paper conducted an extensive literature review by exploring relevant articles from five major academic databases (IEEE Xplore, Web of Science, ACM digital library, INSPEC, and ScienceDirect) to clarify and to understand the current status and the potential research directions regarding the issues of cybersecurity in IoT. Our review identifies cybersecurity countermeasures and the techniques of IoT that have been employed in diversified industries and highlights the challenges and opportunities for other interested researchers. According to the five databases, there exist a large number of journal articles and conference papers related to IoT cybersecurity. For this research, for example, 433 articles (IEEE Xplore) from 2013 were chosen. The trend in Figure 1 illustrates that cybersecurity is becoming a hot issue in IoT research.

II. IoT-BASED CYBERSECURITY MANAGEMENT SYSTEM

IoT integrates heterogeneous smart devices into an integrity network. IoT cybersecurity is a mechanism for the strategic improvement of, and encompasses all of the changes involved, in IoT, to ensure the safety of the entire environment.

A. Cybersecurity-Oriented IoT Architecture

In Table I, the popular IoT cybersecurity architectures from different perspectives are listed. The table clearly illustrates that scholars construct IoT cybersecurity frameworks into three major categories: basic three-layer architecture, derived four-layer architecture, and detailed five-layer architecture. The layers are the perception (sensor) layer, the accessing layer, the network layer, the middleware layer, the application (service) layer, and the interface layer.

Table I
SUMMARY OF DIFFERENT IOT ARCHITECTURES

Number of Layers	Major Technologies	Article
Three Layers	Sensing, Network, Application	[2]
	Perception, Network, Application	[14]
	Perception, Transportation, Application	[15]
	Perception, Network, Application	[16]
	Perception, Network, Service	[17]
	Perception, Network, Application	[18] [33]
Four Layers	Sensing, Networking, Service, Interface	[1]
	Perception, Network, Support, Application	[7]
Five Layers	Field Data Acquisition, Access Gateway, Internet, Middleware, Application	[3]
	Perception, Network, Middleware, Application, Business	[19]

An IoT architecture was proposed by [2] that includes three fundamental layers: the application layer, the network layer, and the sensing layer. From a service-oriented view, [1] divided the whole framework into four layers, based on the SOA (service-oriented architecture): the sensing layer, the network layer, the service layer, and the interface layer.

Moreover, the IoT architecture from other studies is described below. For instance, for the three-layered architecture, most studies [14]-[18] have the same architecture as Atzori's. In the four-layered architecture, as compared to Xu's architecture, the third layer constructed by [7] is the support layer, which is especially for cloud computing. For the five-layered architecture, based on Atzori's architecture, [19] added two more common layers: the middleware and business layers. [3] proposed a five-layered generic IoT architecture that

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2869847, IEEE Internet of Things Journal

can satisfy various industries. The two bottom layers the field data collection layer and the access gateway layer process data collection, the Internet layer serves communication media, and the two top layers (the middleware layer and the application layer) are responsible for data utilization.

The architectural design of IoT-based cybersecurity is concerned with architecture protocols, wireless networking and communication, principles and functionalities, heterogeneous and ubiquitous devices, authentication, lightweight technologies, etc. From the technological perspective, the design of the architecture requires accessibility, integrity, availability, scalability, confidentiality, and interoperability among heterogeneous smart devices [20]. From the hardware/software limitations, the design of the architecture should be used in conjunction with computing and energy, memory, tamper-proof packaging, embedded software, and dynamic patches. Since cybersecurity might change or might need real-time interaction within the related environment, an adaptive architecture is needed to assist devices which dynamically interact with other things in IoT. At each layer, IoT devices and services are vulnerable to malicious attacks that can disrupt or destroy IoT network and services. From the perspective of cybersecurity, a four-layered IoT architecture (Table II) is constructed in our study.

TABLE II
A FOUR-LAYERED CYBERSECURITY-ORIENTED ARCHITECTURE FOR IOT

Layers	Description	Attack Types
Sensing	Sensing objects and data. Attack focus: confidentiality	Replay Attacks, Timing Attacks, Node Capture Attacks, Malicious Data Attacks, SCA (Side Channel Attack)
Networking	Networking and data transmission. Attack focus: confidentiality, privacy, and compatibility	Spoofed, altered or replayed routing information, Sybil, Wormholes
Middleware	Data delivery. Attack focus: authenticity, integrity and confidentiality	Malicious Insider, underlying infrastructure, third-party relationships, virtualization threat
Application	Requested service provision. Attack focus: data privacy and identity authentication	Phishing Attack, Virus, Worms, Trojan Horse and Spyware, Malicious Scripts, Unauthorized Access

B. The Four Layers and Cybersecurity

The IoT is a global network, in which things or objects can be connected and operated by smart devices such as Radio-Frequency Identification (RFID) tags and readers [21], sensors, actuators, smartphones, etc. At each layer, IoT-related things are susceptible to Denial of Service attacks (DoS), due to their limited storage capacity, power consumption, and computation capability.

A DoS Attack is an attempt to deny end users access to resources related to the Internet of Things (e.g., machine or network resources). Interference channels, bandwidth, memory, disk space, processor time, and configuration information outages are all potential channels for DoS attacks [4], [22]-[24]. A DoS attack has two types: Distributed Denial of Service (DDoS) and Ordinary DoS [25].

1) The Sensing Layer

The sensing layer, which consists of data sensors and networks, can detect, collect, process, and transmit information or data to the entire network [1]. There exist three major cybersecurity issues at this layer: (1) the strength of wireless signals, (2) the exposure of sensor nodes in IoT devices, (3) the dynamic nature of IoT topology, and (4) communication, computation, and storage and memory constraints [26].

This layer employs three popular mechanisms to protect the IoT network: the lightweight encryption mechanism, the access control mechanism, and the nodes authentication mechanism. In practice, many attacks and crimes, such as Replay Attacks, Timing Attacks, Node Capture Attacks, Malicious Data Attacks, and others, focus on the confidentiality of the perception layer.

A Replay Attack is made by spoofing, altering, or replaying the identity information of smart devices in the IoT network. A Time Attack is an attacker stealing the encryption key associated with time and other important information [27]. A Node Capture Attack is when an attacker takes over nodes and captures useful information and data. In addition, the attacker can send Malicious Data to the layer by adding another node to the network [26]. A Side Channel Attack (SCA) refers to an attack on the side leakage information (such as time consumption, power consumption or electromagnetic radiation, etc.) of the encryption device, through the operation process of the device [14].

As an example, Hanney needs to prove her identity to Jerry to access a web account. Jerry requests her password as proof of identity, and it is provided by Hanney. At the same time, Jack is eavesdropping on the conversation and saves the password. Later, Jack shows the password to Jerry as proof of access to Hanney's website account.

2) The Network Layer

The network layer serves the function of data routing and transmission to different IoT hubs and devices over the Internet and the mobile network [2]. At this layer, cloud computing platforms, Internet gateways, switching, and routing devices are operated by using some of the very recent technologies such as WiFi, LTE, Bluetooth, 3G/4G, Zigbee etc. The network gateways serve as the mediator between different IoT nodes by aggregating, filtering, and transmitting data to and from different sensors.

Confidentiality, privacy, and compatibility are the main cybersecurity issues at this layer. In the IoT global network, the interactive function may be human-to-machine, machine-to-human, human-to-human, or machine-to-machine. The interconnection is handled by wired or wireless mechanisms among heterogeneous smart devices. Because everything is embedded in the IoT network, attackers have a good chance of evincing criminal activities. Specifically, the network layer is very vulnerable to a type of attack called a Man-in-the-Middle attack. Advanced protocols and software/hardware can detect

abnormal behaviors or situations to keep IoT secure [28], [29]

Spoofing, modification, and replay are mutual direct attacks that target data exchange, generate fake and false messages, and create routing loops between nodes. A Sybil attack is a single node that can be located at multiple locations at the same time across multiple identities. Sybil attacks steal information by spreading malware, reducing integrity and resource utilization within the Internet of Things. Social media such as Facebook and Twitter are vulnerable to Sybil attacks [30].

As an example, an attacker can contaminate the entire network by sending fake routing information. On Twitter, a user is asked to do a survey before allowing him/her to enter the fake Twitter login page. As the user logs in, the fake page can record the user's credentials, display the login error, and redirect the user to the real Facebook page. During this operation, the user's information can be stolen.

3) The Middleware Layer

The middleware layer is based upon the principle of Service Oriented Architecture (SOA) [2]. It is a software layer between network and application levels. At this level, the authenticity, integrity and confidentiality of all of the exchanged data needs to be operated and managed. Through the Internet of Things architecture, intelligent middleware can combine high spatial-temporal resolution with the ubiquitous nature of sensor networks and other identifiable things to create dynamic mechanisms for the physical world in the digital/virtual world [31].

A Malicious Inside Attack is the internal attackers deliberately modifying and extracting data or information within the network [32]. An Underlying Attack is a platform-as-a-service (PaaS) based attack. The goal of developers is to maintain the secure application of IoT, and to maintain the security of the lower layers [33]. Third-party relationship attacks are caused by third-party components such as mashups, which increase the security of data and networks on PaaS [34]. A virtualization attack means that a virtual machine may be damaged and may affect other virtual machines. Many different types of attacks may occur [35].

For example, assume that an insider illegally accesses a system or a network and investigates the nature of system or network to target vulnerable points. Then, a workstation may be executed to leak or to destroy data or information.

4) The Application Layer

According to standardized protocols and service technologies, the application layer explores all system functionalities for the final users [1].

In the application layer, malicious data is shared and exchanged among smart devices. How to protect data privacy and security and how to identify objects depending on non-standard authentication mechanisms are big challenges to practitioners and to scholars [16]. Common security problems in this layer are (1) data access permissions, identity authentication, (2) data protection and recovery, (3) the ability of dealing with mass-data, and (4) software vulnerabilities [14].

A Phishing Attack is done by an attacker who obtains useful information or data from the user by stealing an authentication authorization, such as login credentials, credit card information [32]. The attacker injects malware into the system through viruses, worms, Trojan horses, and spyware to deny service, change data, and/or access confidential data [36]. When the user monitors the gateway and runs the Active-X script, the system shuts down. Attackers can control access and steal data [37]. In an Unauthorized Access Attack, an attacker can easily cause damage to the system by forbidding access to related services of IoT or by deleting existing data.

C. Attack Taxonomy

Due to the heterogeneity of smart devices, communication protocols, applications, and services, the attacks appear to be malicious. We categorize different attacks into eight classifications [13]. Details are in Figure 2.

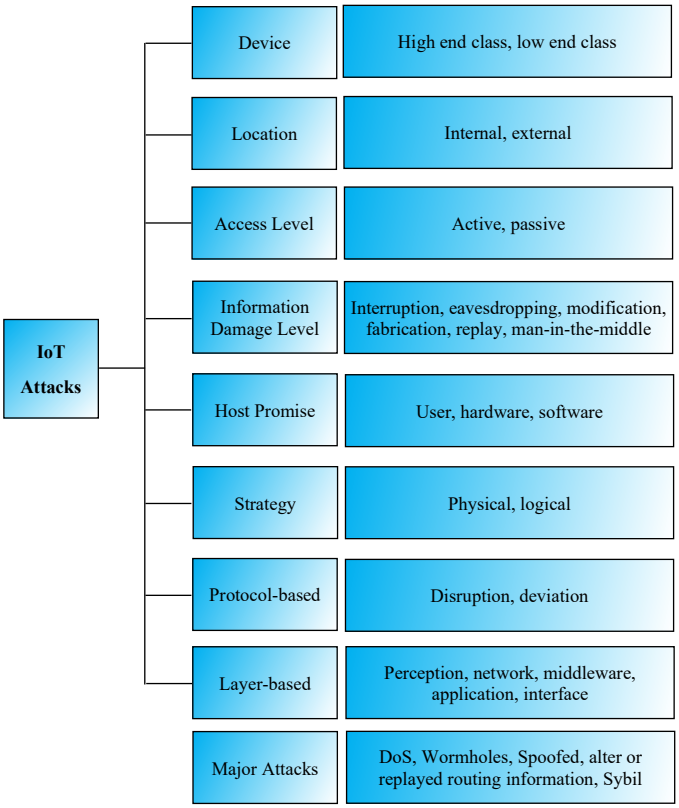

Fig. 2. Taxonomy of Cybersecurity Attacks on IoT

Attacks Based on Devices are high-end and low-end device attacks. Attacks Based on Location are internal and external attacks. Attacks Based on Access Level are active and passive attacks [38]-[40]. Attacks Based on Information Damage include interruption, eavesdropping, modification, fabrication, replay, and man-in-the-middle attacks. Host-Based Attacks are users, hardware, and software attacks. Attacks Based on Strategy are physical and logical attacks. Protocol-Based Attacks are disruption and deviation attacks. Layer-Based Attacks are perception, network, middleware, and application attacks.

High-end device attacks involve high-power/full-fledged devices to launch attacks on the IoT system, while low-end device attacks involve low power devices to attack the IoT system [41].

Internal threats ("Insider") originate from inside the IoT network, and external threats ("Outsider") originate outside the IoT network [42]. In an internal attack, the attacker attempts to execute his own malicious code on smart devices in the IoT network. There are four types of internal attacks in practice: affected roles, unintentional roles, emotional attackers, and technically aware roles. An attacker tries to randomly, and without the user's knowledge, access IoT smart devices outside the network, remotely.

Without disrupting information and communication in the IoT network, passive attacks involve monitoring and eavesdropping to recover information [26], [43]. Contrary to passive attacks, active attacks directly affect the communication system in the IoT networks. Active attacks can circumvent or destroy smart devices and can destroy information or data [44], [40].

The focus of the Interrupt Attack is on interrupting the availability of the system. If this occurs, resources will be exhausted and smart devices may shut down [7], [45]. Eavesdropping on the communication channel prevents the receiver device from selecting packets to send. RFID devices are vulnerable to eavesdropping attacks [46]. Attacks can alter or modify information or data in the IoT smart devices to mislead the communication protocol. This attack threatens the integrity of the IoT network security requirements [47]. A Fabrication Attack occurs when an attacker inserts counterfeit data into the IoT architecture to create damage to the IoT information system and to threaten IoT authentication [43].

Credential information or data (such as passwords or keys) associated with actual users may be misappropriated and abused [48]. Attackers attack software because of IoT device exhaustion or resource buffer overflow vulnerability [49]. Attackers injecting malicious code or stealing the actual driver or connecting to the device is a Hardware Attack [50], [51].

Since most smart devices are run in an outdoor environment, physical attacks are likely to tamper with hardware. Physical attacks are similar to hardware attacks. Logical Attacks bring dysfunction to communication systems over the IoT network without harming physical devices [52].

Attackers can attack IoT in an abnormal manner. External attackers may pretend to be insiders and may execute malicious code on the IoT network. Thus, attackers can attack protocols by disrupting internal or external networks: key management protocol, data aggregation protocol, synchronization protocol, etc. Deviation Attacks have two target protocols: application protocol and the network protocol [39].

III. Key Enabling Measurements

The IoT is susceptible to various security attacks by hackers or behavioral criminals. Many researchers [53] have explored the IoT security countermeasures from layer-level perspectives. At each layer, the related attacks and countermeasures are described. But so many objects, attacks, and countermeasures are spread across the dynamic network. For instance, DoS attacks appear at most layers of the IoT network via malicious attacking perspectives, and RFID devices use different countermeasures to deal with attacks throughout IoT. Hence, in this section, we briefly introduce some common countermeasures that apply not only to different layers but also to smart devices, intelligent objects, and the entire network. RFID (Radio Frequency Identification) and WSNs (Wireless Sensor Networks) are the two fundamental technologies for the creation and development of IoT. Moreover, technological device-involved measures and security schemes are illustrated in detail.

A. RFID-based Authentication Measures

RFID technology allows the microchip to transmit identification information to the reader through wireless communication. By using RFID devices, people and entities can identify, track, and monitor any object that has an RFID tag or label attached. RFID has been widely used in transportation systems, medical records, and supply chain management [54]. RFID and the related technologies and instruments will be the cornerstone of the upcoming Internet of Things, even as Radio Frequency Identification techniques (RFID) and the related technologies make IoT more feasible and riskier, especially when one considers possible application for authentication in the IoT global network.

RFID devices tag or label each device to enable identification mechanisms in the IoT network. Authentication is a necessary and viable connection between two things to prevent data attacks. Specifically, RFID cybersecurity measures include (1) access control, (2) data encryption, (3) IPSec-based security channels, (4) cryptography technology schemes, and (5) physical cybersecurity schemes.

Access control is a mechanism to prevent attackers from stealing or misusing RFID devices' information or data, such as label failure, chip protection, and antenna energy analysis. Data encryption is a mechanism that encrypts RFID signals and prevents data privacy through an algorithm. This algorithm also prevents attackers from eavesdropping and tampering with data during transmission. The IPSec-based secure channel integrates IPSec protocols and security mechanisms to perform authentication and encryption over the IoT network. Based on secure communication protocols (hash function, random number mechanism, server data search, logic algorithms, and re-encryption mechanisms), cryptographic technology solutions primarily protect user privacy, in addition to the confidentiality, authenticity, and integrity of RFID systems. Physical security schemes can be divided into two categories: hiding and masking. The hiding schemes eliminate the data dependencies of the energy consumption; the masking schemes randomize the intermediate values of the encryption devices [14].

B. WSN-based Measures

Wireless Sensor Network (WSN) technology uses interconnected smart devices for sensing and monitoring. Its applications include environmental monitoring, medical monitoring, industrial monitoring, traffic monitoring, etc. [55], [56].

Data and information are collected and transmitted through WSN, in which attackers actively and aggressively attack

WSN-related data or things. Therefore, it is recommended that many appropriate protection measures be taken to deal with different attacks.

(1) Key Management. With WSN, the appropriate algorithm can be built, and security keys will be generated and updated. Common activities are to forward, backward, and extend privacy, in order to protect collusion attacks and to identify authentication. There are four protocols used: simple key distribution protocols, key pre-distribution protocols, dynamic key management protocols, and hierarchical key management protocols. (2) Secret Key Algorithms. Key algorithms include symmetric and asymmetric key algorithms. Symmetric key algorithms use Skipjack and RC5. Asymmetric key algorithms use RAS (Rivest-Shamir-Adleman) and ECC (Elliptic Curves Cryptography) [57], [58]. (3) Security Routing Protocol. Secure routing protocol algorithms typically use the following mechanisms: clustering mechanisms, data fusion mechanisms, multiple hops routing mechanisms, and key mechanisms. The SPINS security framework protocol is widely used in secure routing technologies and includes the SNEP (Secure Network Encryption Protocol) protocol and μTESLA (Micro Timed Efficient Streaming Loss-tolerant Authentication Protocol) protocol [59]. (4) Authentication and Access Control. Authentication technologies include lightweight public key authentication technology, PSK (Pre-Shared Key), random key pre-distribution authentication technology, auxiliary information authentication technology, and one-way hash function authentication technology. Access control includes asymmetric symmetric cryptosystems. (5) Physical Security Design. Node design and antenna design are the two aspects. Node design consists of hardware structure design and security chip selection, chip connection, radiofrequency circuit design, and data acquisition unit design. Antenna design needs to be suitable for good communication distance, high adaptability, stability, and so on.

C. Security Schemes

In this section, we briefly summarize the IoT security schemes into three categories: Host Identity Protocol (HIP)-based schemes, Datagram Transport Layer Security (DTLS)-based schemes, and Capability-based Access Control (CapBAC) schemes. The advantages and disadvantages of the specific schemes are addressed and discussed as well. An evaluation chart is depicted in Figure 3.

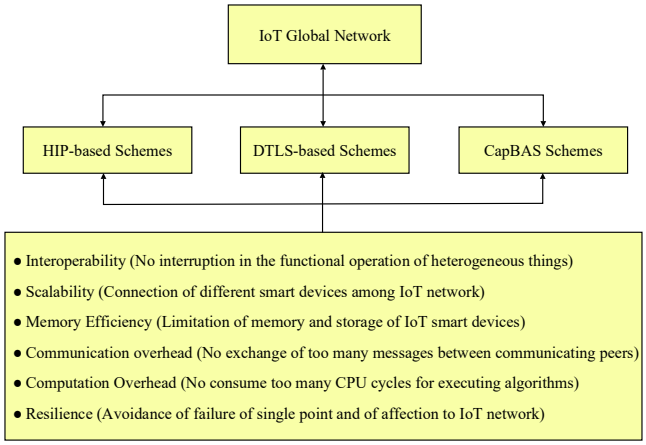

Fig. 3. An Evaluation Chart for IoT Security Schemes

1) Host Identity Protocol (HIP)-based schemes

Based on device mobility security attributes, these schemes, such as interoperability, scalability, memory efficiency, communication and computation overhead, and resiliency, are applied to the authentication of IoT devices [60], [61].

HIP-DEX [62] and Slimfit [63] use Elliptic Curve Diffie-Hellman (ECDH) for key exchange in non-collaborative scenarios, while HIP-TEX [60] employs cryptographic computations of the key exchange in a collaborative environment. HIP-TEX is relatively efficient in terms of computation and memory, but lacks communication efficiency, because HIP-TEX will lead more IoT traffic. Slimfit may be suitable for IoT because it has the advantages of resiliency, memory, and communication skills, but Slimfit does not provide scalability and interoperability. HIP-DEX may be well-suited for IoT with its high computational complexity, since it can achieve high levels of interoperability, resiliency, scalability, communication complexity, and memory.

2) Datagram Transport Layer Security (DTLS)-based schemes

Based on a new standard for the IoT [64], DTLS-based (Datagram Transport Layer Security) schemes were proposed to secure the IoT network. Similar to HIP-based schemes, DTLS-based schemes need to satisfy the attributes of interoperability, resiliency, scalability, communication, memory, and computation.

An X.509-certificate-based DTLS scheme was constructed [65] to mutually authenticate smart devices in IoT but ignoring either to process a certificate chain or to check a revocation list. The delegation-based DTLS schemes [63] utilized a trusted entity Delegation Server (DS) to handle certificate verification in a home network. The certificate-based DTLS schemes facilitate interoperability, resiliency, and scalability, but lack computation, communication, and memory. In contrast, the delegation-based DTLS schemes have the advantages of communication, computation, and memory. However, the delegation-based schemes are vulnerable to single points of failure and to DoS attacks.

3) Capability-based Access Control (CapBAC) schemes

The mechanism for restricting access to authorized users in

IoT is Capability-based Access Control (CapBAC) [66]-[69]. CapBAC uses a cryptographic token to protect access rights and privileges. The CapBAC schemes have two classifications: the centralized approach, which explores the access control logics into a central entity in Cloud, and the distributed approach, which embeds the access control logics into IoT smart devices. The centralized schemes include XACML, SAML based schemes, Kerberos, RADIUS based schemes, OAuth based schemes, and Context-aware schemes, and the distributed schemes include Proxy Assisted schemes, Embedded PDP, etc.

A centralized approach fulfills the requirements of interoperability, computation complexity, and memory efficiency. However, the communication between smart devices and the external entity has to be overloaded. On the other hand, a distributed approach has good level of scalability, but lacks interoperability and memory efficiency [39].

IV. Key Applications in Industries

The IoT makes full use of things, like smart devices and data from the physical world, in a global network, in order to provide secured services to end-users. The IoT cybersecurity system will bring tangible benefits to all walks of life. The more interactions and interoperability, the higher the standard mechanisms and services, the more life-cycle management, and the better the collaboration between companies. Industry relies heavily on control systems, sensor equipment and data networks. The disadvantages of this trend have led to an increase in the number and the types of cybersecurity threats. Cybersecurity attacks against infrastructure and systems have become commonplace in various industries, among medical services, smart cities and home design, and transportation and parking systems.

A. Healthcare Service Industry

The basic characteristics of IoT are the comprehensive recognition of information, reliable delivery of information and smart processing of information. The development of IoT has promoted the informationization process of the medical system. The application of IoT technology in the medical field will improve the cooperation and integration of traditional information technology in the healthcare industry [1], [2].

IoT cybersecurity in the healthcare industry is associated with medical information, identification, hospital emergency, remote monitoring and home care, drug and production supervision, medical equipment and medical waste tracking, blood management, infection control and many more [70]. For example, traditionally medical information needs to be manually entered to generate information, networks, and individual functions. Each department and participant are relatively independent, and information is asymmetry. IoT technology completely breaks these limits with its terminal scalability and accessibility. It enables healthcare systems to more effectively improve overall information levels and collaborate on a variety of service functions.

In the healthcare environment, wireless wearable devices can use IoT-derived data and information to improve basic operations and to become more cost-effective tools [71]. Cybersecurity attacks directly threaten the confidentiality, integrity, and availability of healthcare systems, and include DoS attacks, remote brute force attacks, man-in-the-middle attacks, password sniffing, Trojan horses, and data tampering. [72] addresses the security and privacy challenges faced by eHealth wireless technologies and eHealth smart devices.

With the widespread use of IoT technology in healthcare, new security and privacy issues have arisen. It allows for data privacy, reliability, integrity, and unauthorized identification and tracking of objects. For example, an intruder can use an interfering signal to block an infinite communication line between an RFID tag and a reader in IoT, or even spoof an RFID tag to send an error message to the reader. This will lead to confusion in the medical information system and seriously affect the safety of patients. With the development of IoT and the related technologies, medical care will develop into intelligence, electronic information, artificial intelligence, personalization and mobility [19].

B. Smart Domain

IoT has connected people to things, like smart homes, smart cities, smart meters, smart devices, smart appliances, and social networks. IoT will bring unprecedented improvements in quality of life. One of the goals of IoT is to develop smart environments and self-conscious/autonomous objects: smart transport, smart cities, smart homes, smart health, smart living, and so on [73], [74].

Cybersecurity includes illegal access to information and attacks, resulting in a disruption of service availability. Data privacy and emergency responses trigger technical challenges in smart environments. For cybersecurity purposes, the IoT infrastructure needs to be confidential, auto-immune, and reliable, in order to protect and to improve the smart environment. For example, in a smart home, only authorized users can monitor all the IoT-related smart devices. The password for IoT-related smart devices should be kept confidential. Auto-immunity protects a family from potential intruders through an alarm [75].

A smart home is a collection of devices that make up a variety of smart system. A dynamic heterogeneous architecture is built through the awareness layer, the network layer and the application layer. In the smart home system architecture based on IoT, there is a unified operating standard between the universal IoT devices. The IoT device organization system connects to the access center without directly accessing related devices. Wireless communication methods are commonly used between IoT devices and access centers. Users can interact and manage with IoT devices through different platforms. For example, a personal computer. Commonly used interaction methods are: directly interacting with the device through the access center; connecting to the Internet center through the Internet cloud service [73].

C. Transportation and Parking System

The Transportation IoT was proposed in the context of the development of IoT. In the context of the application of IoT-

related technologies. It can establish the whole process of vehicle tracking, traffic safety and efficiency, intelligent management of urban traffic, and automatic acquisition of more abundant road condition information by vehicles to achieve automatic driving [76], [77].

IoT technology brings a new revolution in transport and logistics systems. The intelligent transportation system will provide efficient traffic control and management in IoT. IoT-based infrastructure and systems can be used to prevent electronic toll collection, mobile emergency command and dispatch, traffic enforcement, vehicle violation monitoring, environmental pollution reduction, and anti-theft systems; and to avoid traffic jams, traffic accidents, intelligent beacons; and to minimize arrival delays [76], [77].

These applications are only part of IoT and have not yet formed a huge network. In the future, intelligent transportation will be accomplished through the connection between vehicles and vehicles, the interaction between people and vehicles, and the huge vehicle connection network. The transportation problems such as traffic congestion, environmental pollution and safety accidents will be appropriately solved [1], [2].

V. Research Challenges & Future Trends

The global IoT network comprises a variety of devices and applications. But, due to different scenarios and requirements, these things may not be designed primarily for security issues. Many challenging issues still need to be addressed in order to achieve a higher level of IoT cybersecurity, e.g., secrecy, confidentiality, data integrity, authentication, access control, etc. Several technologies, standardization, and other emerging research are currently under way, to meet the high standards of IoT cybersecurity. IoT is a network system that connects things based on the internet, and establishes information sharing and exchange. The core of IoT is to achieve convenience, efficiency, and intelligence. The realization of IoT technology is based on infrastructure and high-end technology [78].

A. Standardization

Because of the complex structure of things in IoT, standards and protocols need to be modified and federated with heterogeneous things. A standardized IoT architecture comprising data models, interfaces, and protocols can support a broad range of humans, devices, languages, and operating systems to achieve common goals [16], [28].

The Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF) are the main entities that design new communications and security protocols; they will play an important role in protecting the global IoT network [79], [80]. Table III lists standards and protocols in details.

Table III
STANDARDS & PROTOCOLS FOR IOT CYBERSECURITY

Standards	Security Issue	Application
IEEE 802.15.4 (Perception Layer)	Confidentiality, Integrity, Authentication, Replay attack	Access control mechanism, Time-synchronized communications
6LowPAN (Network Layer)	Confidentiality, Integrity, Authentication, Non-repudiation	Transparent end-to-end security, communications between 6LoWPAN devices
RPL (Middleware Layer)	Confidentiality, Integrity, Authentication, Non-repudiation, Replay attack, Key management	Protecting routing control messages, protecting routing operations against falsified routing updates
CoAP (Application Layer)	Confidentiality, Integrity, Authentication, Non-repudiation, Replay protection	Protecting CoAP application-layer messages, transparent and granular end-to-end security

IEEE 802.15.4 [81], [82] sets the basic rules for lower-level communications and lays the foundation for higher-level IoT communication protocols. 6LoWPAN [83]-[85] supports the transmission of IPv6 packets over IEEE 802.15.4 and implements packet fragmentation and reassembly mechanisms and other functions. The Low-power and Lossy Networks (RPL) [86] proposed by the IETF's Low-Power, Lossless Network Routing (ROLL) Working Group design routing solutions for IoT applications. RPL provides a framework for specific types of applications. The Constrained Application Protocol (CoAP) [87], currently being designed by the Constrained RESTful Environments (CoRE) Working Group of the IETF, supports communications at the application layer.

In fact, we do not have a standardized framework that can integrate data models, ontology, and data formats with IoT protocols, applications, and services. Due to the extant differing standards, more thorough and generalized infrastructure needs to be built to fulfill the interoperability and integrity of IoT mechanisms, applications, and services.

IoT system is such broad platform that consists heterogeneous data, devices, technologies, and protocols. Standardization may be a Garden of Eden that cannot achieve in IoT systems at least in short-term. However, standardization can be the ultimate goal that improves and prompts the development of security in IoT. The following is good examples that company or organization implements standardization issues for both security and IoT.

B. Data Issues

The vast amount of data generated by the Internet of Things in various businesses, including personal basic information, user account transaction data, medical insurance records, and work business information. Once these data are leaked, it will have a major impact on people's lives and work [78]. Malicious data (e.g., personal information, stock data, and medical records) needs to be processed in the IoT network. Data is one of the promising cybersecurity issues in different layers of IoT cybersecurity infrastructure. The major issues are data confidentiality, data privacy, and data integrity. Many approaches have been developed to protect information and data security within the IoT network [77]. Data confidentiality is one of fundamental data issues in IoT cybersecurity. A well-configured scenario guarantees that authorized entities can access and process data and prevents the invasion of unauthorized entities. The two important cybersecurity

mechanisms are access control and the authentication process [76].

Many access control techniques have been proposed, from the previous literature, to ensure confidentiality in IoT. One standard approach is Role-Based Access Control (RBAC). RBAC integrates with real-time and dynamic data streams management systems in IoT to ensure data authenticity, confidentiality, and integrity during transmission [88]-[90]. The second mechanism is a key distribution scheme, that is, secure data aggregation in wireless sensor networks such as SEDAN [91] and SAWAN [92]. In addition, in order to avoid unauthorized access, anonymization techniques based on data suppression, randomization or cloaking have been proposed [93], [94].

Privacy in data collection, sharing, and management open new research issues in IoT. RFID-related devices and technologies are one viable way to protect data security. Many mechanisms have been proposed to address data privacy issues in IoT cybersecurity, such as Kaos [95], Tropos [96], NFR [97], GBRAM [98], PRIS [99]. In addition, security mechanisms, like Data Encryption (RSA, DSA, BLOWFISH and DES) and Biometric Verification, can prevent unauthorized users from accessing data [47]. Data integrity refers to the protection of information or data from attacks or external influences during transmission and reception, maintaining the originality, accuracy, and unfalsification of data [2]. The security mechanisms are Cyclic Redundancy Check (CRC) and Version Control. Data availability ensures that authorized users access their information resources in both normal and abnormal conditions. A Denial-of-Service (DoS) Attack is one of the popular attacks that cybersecurity should focus on. Most functional devices have a more or less security risk. For example, the car's central control display system, webcam, home alarms, etc. IoT devices do not focus on enhancing the security of data information in all aspects of access, transmission, and storage of data information, but are always concerned with the capabilities of the extended device. Traditional security models cannot adapt to new security challenges and the age of information data brought about by IoT. Security issues directly affect the further development and application of IoT. Data security and disposal are issues that cannot be avoided by security issues [1].

The rapid development of big data and IoT has brought convenience to people, and we also encounter unprecedented information security risks [100]. As early as July 2015, American auto companies recalled more than one million vehicles using the Uconnect system. The reason is that there are large security holes in the in-vehicle system. Hackers can use these vulnerabilities to remotely control the onboard system to shut down the engine, accelerate and decelerate the vehicle, and cause brake failure. Due to the virtual nature of IoT, its operating mode relies on the collection and processing of data resources. Currently, IoT and big data technologies combine multiple services. For example, wireless communication technology (Bluetooth, WI-FI, ZigBee), hardware, device and applications, mobile applications, cloud services. On the mobile side, the mobile application is first downloaded by the mobile device (eg, a mobile phone) and communicated with the cloud or sent directly to the terminal device, then forwarding the control commands to the device terminal. In this way, smart devices in IoT can be controlled in any situation that may interfere with the internet, thereby enabling intelligent operations related to data [100].

C. Research Trends

The IoT is an emerging technology that changes all of aspects of society, both for people and for business. With the advance of IoT, many advanced technologies and mechanisms are being initiated.

1) Cloud service security

Cloud computing is based on distributed computing, parallel computing, grid computing and virtualization. Cloud computing can provide massive information storage and analytics for IoT. With the development of IoT, how to analyze and process a large amount of data and information is a real problem. One potential solution is to integrate cloud computing into IoT system. Using cloud computing to build an IoT platform can reduce costs and achieve efficient calculation and storage [101]. Cloud computing provides a high-quality and reliable architecture for IoT and is conducive to the massive expansion of IoT. However, because the cloud computing platform is a relatively open platform, there are many security risks in its operation procedure.

There is a tendency for IoT systems and services to be removed and hosted on cloud platforms, so that devices and applications can be accessed at anytime from anywhere, without boundaries. Smart devices can be deployed and linked to cloud services through Wi-Fi and wireless Internet connectivity systems. The IoT relies on cloud services such as Storage-as-a-Service (SaaS) and Database-as-a-Service (DaaS) to store sensor data [102]. However, cybersecurity concerns have increased. Ways to integrate and improve the existing IoT systems and mechanisms in order to prevent attacks toward cloud-based IoT services will attract more and more attention. Cloud security includes technologies, security controls, and strategies developed for protecting cloud databases and services such as infrastructure (IaaS) platform (PaaS), software (SaaS), and infrastructure (IaaS).

The big data of IoT is stored in a server with a cloud computing platform. Cloud computing servers are distributed around the world. The diversity and complexity of the server determines that the user does not know where the data is stored, and the security risks exist. Cloud computing mainly uses virtual technology to achieve data sharing, and many virtual machines share one resource. Once encryption or isolation of one piece of data is not achieved, the data is transparent and easily exploited by illegal users. The cloud computing platform does not guarantee the complete security of end-user information. The end-user is handed over to the cloud computing platform. Cloud computing platforms analyze and process data and have data access. In this way, the end-user doesn't have complete control over the data. In the process of calculating and processing data in the cloud, the data is easily leaked. There are also security risks in transmitting and using

data in IoT systems [103].

Establishing a secure network environment. A trusted cloud computing platform provides supercomputing capabilities for data storage and web applications. The security measures of the cloud computing platform, such as physical security, system security, network security, database security, etc., ensure the basic computing power of the platform and protect cloud-related end-user's data security and privacy from the unauthorized access and potential threats. Encryption technology is used to protect data. Encryption is a way to handle secret locks and passwords efficiently. Cloud computing-based IoT systems, encryption technologies, authentication and access, and anonymous algorithms will be the means to protect data security and privacy in the near future [103].

2) 5G

The key technologies of 5G are wireless technology and network technology. Wireless technologies include massive MIMO technology, multiple access technology, ultra-high-density network technology, multi-carrier technology and modulation coding technology. Network technologies include network slicing technology, mobile edge computing technology, control plane/user plane separation technology and network function reconstruction technology [104].

With the development of connectivity technology and the integration with smart devices, 5G will enhance the ubiquity, reliability, scalability, and cost-effectiveness of seamless global IoT [104]. Because of more IP identifiable objects, IPv6 is replacing IPv4 to implement IoT, since more bandwidth is needed to solve more traffic issues and delays. Hence, the new generation of communication (5G) has been created and can provide speed between 10-800Gbps, while the current technology (4G) has only provided at a speed of 2-1000 Mbps. 5G technology can also integrate both IPv4 and IPv6. The implementation of 5G will enhance many technologies: Heterogeneous Networks (HetNets), Software Defined Networks (SDNs), Massive MIMO, and Multiple Radio Access, etc. [105], [106]. The development of mobile devices and smartphones enables users to achieve exponential data flow. [107] depicts the use of small cells (e.g., femtocells) in an IoT environment. Femtocell will integrate voice, video and data for mobile users. Proper traffic modeling and deployment strategies will improve the overall performance of femtocell networks in the IoT environment. Furthermore, the Industrial Internet of Things (IIoT) is a rapidly evolving Internet network [24], and embedded sensors are the primary tool for collecting and exchanging data. 5G technology and healthcare systems can be integrated. Users can interact with various types of sensors through a secure wireless medical sensor network (WMSN) [108].

However, as a global dynamic environment, rich source data integrates unlimited systems, and attackers have a great opportunity to identify vulnerable targets and to launch attacks within the IoT network. Cybersecurity issue, such as data privacy, information transmission management, security protocols and mechanisms all need to be considered within IoT interoperability of 5G technology. Mobile communication networks have high security requirements. QoS and industry security mechanisms are key factors in ensuring the high level of security and privacy. The demand for IoT-related services will continue to grow. The core of supporting IoT is a large-scale connection among different things with a delay of about 1 millisecond. The current network has bottlenecks that are difficult to achieve. It is possible for 5G networks to fill this gap, mainly because of the low latency, wide coverage, ultra-dense networks, and large-scale connections of 5G.

*3) Q*oS-based (Quality of service) Design

The ubiquitous IoT requires complex cybersecurity systems to accomplish different tasks. A QoS-based (Quality of Service) cybersecurity infrastructure has the potential to protect and to improve the entire IoT network. QoS research is needed to support the development of IoT. QoS management schemes can improve the levels of RFID system and of cybersecurity infrastructure [109].

Although a lot of research has been done on IoT cybersecurity issues, such as architecture and protocol design, countermeasures, and applications, the quality of service (QoS) in IoT cybersecurity is still an unexplored field of research. Consider, for example, (1) IoT-related resource constraints. QoS-based cybersecurity mechanisms should be simplified in order to solve constraints involved in IoT, such as energy, bandwidth, memory, etc. (2) Data privacy. QoS-based cybersecurity mechanisms should take into account the issue of data privacy, which is critical to IoT security. (3) Scalability. A QoS-based network security mechanism should be able to expand to a large number of sensor nodes and smart devices.

4) Other trends

Fault Tolerance Mechanism The higher the limit on smart devices, the worse the performance of the device, and the more susceptible the devices are to attacks. IoT objects should have certain defensive mechanisms that can be used flexibly when needed and can recover from any possible damage. Hence, fault tolerance is indispensable to cybersecurity [28]. IoT Forensics. Since IoT is a comprehensive definition, crimes such as computer crimes or cloud crimes should be IoT crimes, which involve any abnormal activity or behavior in the IoT paradigm. IoT-related crimes are related to smart devices, services, and communication channels. An effective way to investigate these crimes is to perform digital forensic procedures within the IoT network [39]. Self-Management. One of the ultimate goals of the IoT is to self-manage everything, in order to meet the requirements of different entities (such as people, companies, and institutions). Smart things can be performed without restrictions. For example, smart devices can self-configure, self-maintain, self-repair, and can even play an active role in their own disposal [31]. Blockchain Embedded Cybersecurity Design. The interoperability, integrity, and autonomy of RFID and wireless sensor network technologies, and their low-cost transmission capacity may lead to dynamic system interconnection of distributed resource entities through the IoT network. Cryptography consists of a public key and a private key. The private key needs to be associated with unrelated and constrained objects in the dynamic network. In the long run, smart devices need to be rekeyed in order to ensure the security of information and data [28], [110], [111].

VI. Conclusion

In the Internet of Things (IoT), people, protocols and principles, wireless networking and communication, devices, and technologies collaborate as virtual entities that achieve common goals. The IoT has dramatically changed the entire world and our daily lives. Cybersecurity guarantees that IoT will become a secure network for people, software/hardware, processes, and things. If so, IoT will offer the world a higher level of accessibility, integrity, availability, scalability, confidentiality, and interoperability. At the same time, cybersecurity issues will be one of the primary tasks of IoT in the coming years.

In this article, we have vigorously surveyed the important aspects of IoT cybersecurity, specifically, the state-of-the-art of the current position and potential future directions, the major countermeasures against IoT attacks, and the applications in industries. In addition, we introduced and discussed a possible four-layered IoT cybersecurity infrastructure and a taxonomy of attacks on IoT cybersecurity.

References

[1] L. Xu, W. He, and S. Li, "Internet of Things in industries: a survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233-2243, 2014.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] D. Bandyopadhyay, and J. Sen, "Internet of things: applications and challenges in technology and standardization," *Wireless Pers. Commun.*, vol.58, no.1, pp.49-69, 2011.

[4] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266-2279, 2013.

[5] Gartner (2015). *Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015* [Online]. Available: http://www.gartner.com/newsroom/id/2905717, accessed on Jun. 29, 2018.

[6] D. Evans (2011), "The Internet of things: How the next evolution of the Internet is changing everything," *CISCO*, San Jose, CA, USA, White Paper, Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_ 0411FINAL .pdf, accessed on Jun. 25, 2018.

[7] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," In *Proc. of the Computer Science and Electronics Engineering (ICCSEE)*, vol. 3. IEEE, 2012, pp. 648–651.

[8] M. Covington and R. Carskadden, "Threat Implications of the Internet of Things," In *Proc. of the 5th International Conference on Cyber Conflict (CyCon)*. IEEE, 2013, pp. 1–12.

[9] Y. Lu, "Industry 4.0: a survey on technologies, applications and open research issues," *J. of Ind. Inform. Integ.*, vol. 6, pp. 1-10, 2017.

[10] Helpnetsecurity (2017). *US, China and the UK are top regions affected by IoT security threats,* [Online]. Available: https://www.helpnetsecurity.com/2017/08/16/regions-iot-security-threats/, accessed on Jun. 20, 2018.

[11] NIST (2016), *NIST Cybersecurity for IoT Program*. [Online]. Available: https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program, accessed on Jun. 19, 2018.

[12] KPMG (2017), *Overview of China's Cybersecurity Law*. [Online]. Available: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf, accessed on Jun. 15, 2018.

[13] R. H. Weber, "Internet of things-new security and privacy challenges," *Comput. Law Security Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[14] K. Zhao and L. Ge, ''A Survey on the Internet of Things Security,'' In *Proc. 9th Int. Conf. Comput. Intell. Secur. (CIS)*, Dec. 2013, pp. 663–667.

[15] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, pp. 2481–2501, 2014.

[16] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) Security: Current Status, Challenges and Prospective Measures," In *Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference*, IEEE, 2015, pp. 336-341.

[17] X. Jia, O. Feng, T. Fan, and Q. Lei, "RFID Technology and Its Applications in Internet of Things (IoT)," In *Proc. of the 2nd IEEE International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Apr. 2012, pp.1282-1285.

[18] M. C. Domingo, "An overview of the internet of things for people with disabilities," *J. Netw. Comput. Appl.*, vol.35, no.2, pp.584-596, 2012.

[19] F. Alsubaei, A. Abuhussein, and S. Shiva. "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," *Local Computer Networks Workshops (LCN Workshops), 42nd Conference on*. IEEE, 2017, pp. 112-120, doi: 10.1109/LCN.Workshops.2017.72.

[20] S. A. Alabady, F. Al-Turjman, and S. Din, "A novel security model for cooperative virtual networks in the IoT era", *Springer International Journal of Parallel Programming*, 2018, doi: 10.1007/s10766-018-0580-z.

[21] C. Sun, "Application of RFID technology for logistics on internet of things," *AASRI Procedia*, vol.1, pp.106-111, 2012.

[22] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things," In *Proc. of the Recent Trends in Network Security and Applications*. Springer, 2010, pp. 420–429

[23] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (IACAC) for the internet of things," *Journal of Cyber Security and Mobility*, vol. 1, no. 4, pp. 309–348, 2013.

[24] A. R. Sadeghi, C. Wachsmann, and M. Waidner. "Security and Privacy Challenges in Industrial Internet of Things," *In Annual Design Automation Conference*, ACM, 2015, pp. 54.

[25] A. Belapurkar, A. Chakrabarti, H. Ponnapalli, N. Varadarajan, S. Padmanabhuni, and S. Sundarrajan, *Distributed Systems Security: Issues, Processes and Solutions*. Wiley Publishing, Chichester, UK, 2009.

[26] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)," *Perception*, vol. 111, no. 7, pp. 1-6, 2015.

[27] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146 – 164, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128614003971.

[28] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol.44, no.9, pp.51-58, 2011.

[29] R. E. Crossler, F. Bélanger, and D. Ormond, "The quest for complete security: An empirical analysis of users' multi-layered protection from security threats," *Information Systems Frontiers*, pp. 1-15, 2017, Online published, doi: 10.1007/s10796-017-9755-1.

[30] H. Kumar, D. Sarma, and A. Kar, "Security threats in wireless sensor networks," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 23, no. 6, pp. 39–45, Jun. 2008.

[31] M. Abomhara and G. M. Koien, ''Security and Privacy in the Internet of Things: Current Status and Open Issues,'' In *Proc. IEEE Int. Conf. Privacy Security Mobile Syst.*, May 2014, pp. 1-8, doi: 10.1109/PRISMS.2014.6970594.

[32] S. Li and L. Xu, *Securing the Internet of Things*. Syngress Publishing, Cambridge, MA, 2017.

[33] A. Mukherjee, ''Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality under Resource Constraints,'' In *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[34] K. Hashizume, D. G Rosado, E.Fernández-Medina, E. B. Fernandez, "An analysis of security issues for cloud computing", *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 5, 2013.

[35] K. Nagaraju and R. Sridaran, "A survey on security threats for cloud computing," *International Journal of Engineering Research & Technology*, vol. 1, no. 7, pp. 1-10, 2012.

[36] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.

[37] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jul. 2014.

[38] M. Hossain, R. Hasan, and A. Skjellum, "Securing the Internet of Things: A Meta-Study of Challenges, Approaches, and Open Problems," *Distributed Computing Systems Workshops (ICDCSW), 2017 IEEE 37th International Conference on*. IEEE, 2017, pp. 220-225.

[39] M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the IoT," In *Services (SERVICES), 2015 IEEE World Congress on* IEEE, 2015, pp. 21-28.

[40] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in rpl-based internet of things," *International Journal of Network Security*, vol. 18, no. 3, pp. 459–473, 2016.
[41] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 591–601, 2014.
[42] T.-G. Lupu, I. Rudas, and N. Mastorakis, "Main Types of Attacks in Wireless Sensor Networks," In *WSEAS International Conference, Proc. Recent Advances in Computer Engineering*, no. 9. WSEAS, 2009.
[43] S. Alam and D. De, "Analysis of security threats in wireless sensor network," *International Journal of Wireless and Mobile Networks*, vol. 6, no. 2, pp. 35–46, Apr. 2014.
[44] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, "Different types of attacks on integrated manet-internet communication," *International Journal of Computer Science and Security*, vol. 4, no. 3, pp. 265-274, 2010.
[45] T. Heer, O. Garcia-Morchon, R. Hummen, S. Loong Keoh, S. S. Kumar, and K.Wehrle, "Security challenges in the IP-based internet of things," *Wireless Pers. Commun.*, vol. 61, pp. 527–542, 2011.
[46] G. P. Hancke and S. C. Centre, "Eavesdropping Attacks on High-Frequency RFID Tokens," In *Proc. Workshop Radio Frequency Identification Security*, Jul. 2008, pp. 100–113.
[47] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc networks," In *Proc. 6th Int'l. Conf. Mobile Comp. Net., MobiCom 2000*, Aug. 2000, pp. 275–83.
[48] M. Uma and G. Padmavathi, "A survey on various cyber attacks and their classification", *International Journal of Network Security*, vol. 15, no. 6, pp. 391-397, 2013.
[49] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: opportunities and challenges," *Inf. Sci.*, vol. 305, pp. 357– 383, 2015, doi:10.1016/j.ins.2015.01.025.
[50] A. Perrig, J. Stankovich, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, Jun. 2004.
[51] H. Abie and I. Balasingham, "Risk-based Adaptive Security for Smart IoT in eHealth," In *Proc. of the 7th International Conference on Body Area Networks. ICST*, 2012, pp. 269–275.
[52] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)," *ser. Communications in Computer and Information Science*. Springer Berlin Heidelberg, 2010, vol. 89, book section 42, pp. 420–429. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-14478-3 42
[53] J. P. Walters and Z. Liang, "Wireless Sensor Network Security: A Survey," *Security in Distributed, Grid, and Pervasive Computing*, Ed. Y. Xiao, Auerbach Publishing, CRC Press, 2006.
[54] E. W. T. Ngai, K. K. Moon, F. J. Riggins, and C. Y. Yi, "RFID research: an academic literature review (1995–2005) and future research directions," *Int. J. Prod. Econ.*, vol. 112, no. 2, pp. 510–520, 2008.
[55] S. Li, L. Xu, and X. Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and internet of things," *IEEE Trans. Ind. Informat.*, vol. 9, no. 4, pp. 2177–2186, Nov. 2013.
[56] W. He and L. Xu, "Integration of distributed enterprise applications: a survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 35–42, Feb. 2014
[57] A. Perrig et al., "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, pp. 521–34, 2000.
[58] F. Al-Turjman and S. Alturjman, "Confidential Smart-Sensing Framework in the IoT Era", *The Springer Journal of Supercomputing*, 2018, doi: 10.1007/s11227-018-2524-1.
[59] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Trans. Inform. System Security (TISSEC)*, vol. 8, pp. 41–77, 2005.
[60] Y. B. Saied and A. Olivereau, "D-HIP: A distributed key exchange scheme for HIP-based Internet of Things," in *WoWMoM*, IEEE, 2012, Online published, doi: 10.1109/WoWMoM.2012.6263785
[61] R. Hummen, J. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards Viable Certificate-based Authentication for the Internet of Things," In *Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Security Privacy*, 2013, pp. 37–42.
[62] S. L. Keoh, S. S. Kumar, and O. Garcia-Morchon, "Securing the IP-based Internet of Things with DTLS," WiSec', Apr. 2013 [Online]. Available: https://www.researchgate.net/profile/Sandeep_Kumar95/publication/262210719_Securing_the_IP-based_internet_of_things_with_HIP_and_ DTLS/ links/561e22a808aef097132b3120/Securing-the-IP-based-internet-of-things-with-HIP-and-DTLS.pdf.
[63] R. Hummen, J. Hiller, M. Henze, and K. Wehrle, "Slimfit—A HIP DEX Compression Layer for the IP-based Internet of Things," In *Proc. IEEE 9th Int. Conf. WiMob*, 2013, pp. 259–266.
[64] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained application protocol (CoAP)," *IETF 2013*. [Online]. Available: http://tools.ietf.org/html/draft-ietf-corecoap-18.
[65] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "A DTLS based End-to-End Security Architecture for the Internet of Things with Two-Way Authentication," In *Proc. IEEE 37th Conf. Local Comput. Netw. Workshops*, Oct. 2012, pp. 956–963.
[66] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An oauth-based authorization service architecture for secure services in IoT scenarios," *IEEE Sensors J.*, vol. 15, no. 2, pp. 1224–1234, Feb. 2015.
[67] R. Hummen, H. Shafagh, S. Raza, T. Voig, and K. Wehrle, "Delegation-based Authentication and Authorization for the IP-based Internet of things," in *Proc. 11th Annu. IEEE Int. Conf. Sens., Commun. Netw. (SECON)*, 2014, pp. 284–292.
[68] P. Pereira, J. Eliasson, and J. Delsing, "An Authentication and Access Control Framework for COAP-based Internet of Things," In *Proc. 40th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, TX, USA, Oct. 2014, pp. 5293–5299.
[69] B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability-based Access Control Delegation Model on the Federated IoT Network," In *Int'l Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2012, pp. 604-608.
[70] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, 2012.
[71] S. Li, L. Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol.17, no.2, pp.243-259, 2015.
[72] Omoogun, Michelle, et al. "When eHealth Meets the Internet of Things: Pervasive Security and Privacy Challenges." In *Cyber Security and Protection Of Digital Services (Cyber Security), 2017 International Conference on.* pp. 1-7, IEEE.
[73] C. W. Tsai, C. F. Lai, and A. V. Vasilakos, ''Future internet of things: open issues and challenges,'' *Wireless Netw.*, vol. 20, no. 8, pp. 2201-2217, 2014.
[74] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-things-based smart cities: Recent advances and challenges," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 16–24, Jan. 2017.
[75] A. S. Elmaghraby, M. M. Losavio, "Cyber security challenges in smart cities: safety, security and privacy," *Journal of Advanced Research*, Volume 5, No. 4, pp. 491-497, July 2014, doi: 10.1016/j.jare.2014.02.006.
[76] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," In *Proc. 10th Int. Conf. FIT*, 2012, pp. 257–260.
[77] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, "A Systemic Approach for IoT Security," In *Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on*. IEEE, 2013, pp. 351–355.
[78] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "IoT security: ongoing challenges and research opportunities." In *Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on*, IEEE, 2014, pp. 230-234.
[79] J. Granjal, E. Monteiro, and J. S. Silva, ''Security for the Internet of Things: A survey of Existing Protocols and Open Research Issues,'' *IEEE Commun. Survey Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.
[80] K. T. Nguyen, M. Laurent, and N. Oualha, ''Survey on secure communication protocols for the Internet of Things,'' *Ad Hoc Netw.*, vol. 32, pp. 17–31, Sep. 2015.
[81] IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), *IEEE Std. 802.15.4-2011* (Revision of IEEE Std. 802.15.4-2006), (2011) 1-314, 2011.
[82] IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC Sublayer, *IEEE Std. 802.15.4e-2012* (Amendment to IEEE Std. 802.15.4-2011), (2012) 1-225, 2012.
[83] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, Goals," RFC 4919, 2007, [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc4919.txt.pdf.
[84] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets Over IEEE 802.15.4 Networks," RFC 4944, 2007, [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc4944.txt.pdf.
[85] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams Over IEEE 802.15.4-Based Networks," RFC 6282, 2011, [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc6282.txt.pdf.
[86] T. Winter, et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550, 2012, [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc6550.txt.pdf.

[87] C. Bormann, A. Castellani, and Z. Shelby, "CoAP: An application protocol for billions of tiny internet nodes," *IEEE Internet Comput.*, vol. 1, no. 2, pp. 62–67, Mar./Apr. 2012.
[88] R. Sandhu, E. J. Coyne, H. L. Feinstein, and C.E. Youman, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.
[89] S. Papadopoulos, Y. Yang, and D. Papadias, "CADS: Continuous Authentication on Data Streams," In *Proc. of the 33rd international conference on Very large data bases*, VLDB Endowment, 2007, pp. 135–146.
[90] R. V. Nehme, E. A. Rundensteiner, and E. Bertino, "A security punctuation framework for enforcing access control on streaming data," in *ICDE*, 2008
[91] M. Bagaa et al., "SEDAN: Secure and Efficient Protocol for Data Aggregation in Wireless Sensor Networks," In *Proc. of IEEE LCN. IEEE*, 2007, pp. 1053–1060.
[92] L. Hu and D. Evans, "Secure Aggregation for Wireless Networks," In *Proc. Symposium Applications Internet Workshops*, 2003, pp. 384–391.
[93] T. Mielikainen, "Privacy Problems with Anonymized Transaction Databases," In *International Conference on Discovery Science*, Springer, Berlin, Heidelberg, 2004, pp. 219-229.
[94] A. Narayanan and V. Shmatikov, "Obfuscated Databases and Group privacy," In *CCS'05: Proc. of the 12th ACM conference on Computer and communications security*, 2005, pp. 102–111.
[95] A. van Lamsweerde, "Goal-Oriented Requirements Engineering: A Guided Tour," In *Proc. Fifth IEEE Int'l Symp. Requirements Eng.*, pp. 249-263, 2001.
[96] H. Mouratidis, P. Giorgini, and G. Manson, "Integrating Security and Systems Engineering: Towards the Modelling of Secure Information Systems," In *Proc. 15th Conf. Advanced Information Systems Eng.*, pp. 63-78, 2003.
[97] J. Mylopoulos, L. Chung, and B. Nixon, "Representing and using nonfunctional requirements: a process-oriented approach", *IEEE Trans. on Software. Engineering*, Vol. 18 No. 6, pp. 483-497, Jun. 1992.
[98] A.I. Anton, "Goal Based Requirements Analysis," In *Proc. Second Int'l Conf. Requirements Eng.*, ICRE, 1996, pp. 136–144.
[99] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: the pris method," *Requirements Eng.*, vol. 13, no. 3, pp. 241–255, 2008.
[100] Y. Chen, H. Chen, A. Gorkhali, Y. Lu, Y. Ma, and L. Li, "Big data analytics and big data science: a survey," *Journal of Management Analytics*, vol.3, no.1, pp. 1-42, 2016.
[101] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan, "The rise of "big data" on cloud computing: Review and open research issues," *Information Systems*, 47, pp. 98-115, 2015.
[102] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): a vision, architectural elements, and future directions." *Future gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645-1660, Sep. 2013.
[103] A. Whitmore, A. Agarwal, and L. D. Xu, "The internet of things—a survey of topics and trends," *Information Systems Frontiers*, vol.17, no.2, pp.261-274, 2015.
[104] M. R. Palattella et al., "Internet of things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.
[105] W. H. Chin, F. Zhong, and R. Haines, "Emerging technologies and research challenges for 5G wireless networks," *IEEE Wireless Commun.*, vol. 21, no. 2, pp. 106–112, Apr. 2014.
[106] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 28–35, Sep. 2015.
[107] F. Al-Turjman, E. Ever, and H. Zahmatkesh, "Small cells in the forthcoming 5g/iot: traffic modelling and deployment overview", *IEEE Communications Surveys and Tutorials*, 2018. DOI. 10.1109/COMST.2018.2864779.
[108] F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial internet of things (iiot) healthcare applications", *IEEE Trans. Ind. Informat.*, 2018. DOI. 10.1109/TII.2018.2808190.
[109] L. Li, S. Li, and S. Zhao, "QoS-aware scheduling of services-oriented internet of things," *IEEE Trans. Ind. Informat.*, 10(2), pp. 1497-1505, 2014.
[110] Y. Lu, "Blockchain: a survey on functions, applications and open issues," *J. Ind. Inform. Manag.*, 2018, online published, doi.org/10.1142/S242486221850015X.
[111] Y. Lu, "Blockchain and the related issues: a review of current research topics," *Journal of Management Analytics*, 2018, online published, doi.org/10.1080/23270012.2018.1516523.

Yang Lu (M'18) received his B.S. degree from Jilin University, China, in 2004 and the M.S. degree from the University of Manchester, UK, in 2006. He is currently pursuing his Ph.D. degree in ICT (Information and Communication Technology) in USA. He is a member of IEEE. He has published research papers in refereed journals published by major publishers such as Elsevier, Taylor and Francis, and World Scientific.

Li Da Xu (M'86–SM'11-F'16) received B.S. degree in information science and engineering from the University of Science and Technology of China, in 1978, M.S. degree in information science and engineering from the University of Science and Technology of China, in 1981, and Ph.D. degree in systems science and engineering from Portland State University, USA, in 1986.
He is an IEEE Fellow, academician of the European Academy of Sciences, and academician of the Russian Academy of Engineering (formerly USSR Academy of Engineering). Dr. Xu is a 2016 and 2017 Highly Cited Researcher in the field of engineering named by Clarivate Analytics (formerly Thomson Reuters Intellectual Property & Science).