Journal of Hardware and Systems Security (2018) 2:97–110
https://doi.org/10.1007/s41635-017-0029-7

Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice

Kejun Chen[1] · Shuai Zhang[1] · Zhikun Li[1] · Yi Zhang[2] · Qingxu Deng[1] · Sandip Ray[3] · Yier Jin[3]

Received: 7 November 2017 / Accepted: 17 November 2017 / Published online: 10 May 2018

Abstract

Recent years have seen rapid development and deployment of Internet-of-Things (IoT) applications in a diversity of application domains. This has resulted in creation of new applications (e.g., vehicle networking, smart grid, and wearables) as well as advancement, consolidation, and transformation of various traditional domains (e.g., medical and automotive). One upshot of this scale and diversity of applications is the emergence of new and critical threats to security and privacy: it is getting increasingly easier for an adversary to break into an application, make it unusable, or steal sensitive information and data. This paper provides a summary of IoT security attacks and develops a taxonomy and classification based on the application domain and underlying system architecture. We also discuss some key characteristics of IoT that make it difficult to develop robust security architectures for IoT applications.

Keywords IoT security · IoT taxonomy · Vulnerabilities

✉ Yier Jin
yier.jin@ece.ufl.edu

Kejun Chen
chenkj@stumail.neu.edu.cn

Shuai Zhang
zhangshuai@stumail.neu.edu.cn

Zhikun Li
zhikun12111@stumail.neu.edu.cn

Yi Zhang
zhangyi@bmie.neu.edu.cn

Qingxu Deng
dengqx@mail.neu.edu.cn

Sandip Ray
sandip@ece.ufl.edu

[1] Department of Computer Science and Engineering School, Northeastern University, Shenyang, Liaoning, China

[2] Department of Sino-Dutch Biomedical and Information Engineering School, Northeastern University, Shenyang, Liaoning, China

[3] Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611, USA

1 Introduction

The early years of the Internet-of-Things (IoT) primarily involved data communication through machine to machine (M2M) interactions [1]. However, the concept has evolved rapidly to include human interactions as well, ushering in an era of Internet-of-Everything (IoE). Today, our world includes billions of sensors and computing devices that are continually sensing, collecting, consolidating, and analyzing significant amount of our personal information. Such information may include our location, contact list, browsing patterns, and health and fitness information. The sensing, collecting, and propagating of such intimate personal data by computing devices is primarily motivated by convenience: as devices get smarter, they can react better to our needs, wishes, and even moods (e.g., a home thermostat can adjust temperature based on number of occupants, time of day, day of week, season of year, etc.) and handle emergencies (e.g., a home security system can react to a fire or break-in). Unfortunately, this convenience comes at the expense of security and privacy challenges: the private, personalized information, if accessible to an

unauthorized, malicious agent, can result in significant damage to our wealth, reputation, and personal security. In addition to our own personal data, these devices also include assets introduced by their manufacturers at various stages during their production supply chain. These include fuses, firmware, and debug modes. Unauthorized access to these assets can result in loss of millions of dollars in stolen intellectual properties, as well as potentially dangerous misuse of the assets. With the ubiquitous deployment of these devices, such security vulnerabilities can be catastrophic.

The point of computing devices having such potentially catastrophic vulnerabilities is not merely academic. It can happen—unfortunately too easily in practice. There have been numerous demonstrations of attackers being easily able to inject malicious code directly into wearable devices by using programming interface and then acquire sensitive data of users [2]. There have been demonstrated attacks on implantable medical devices, such as implantable cardioverter defibrillator (ICD) [3], which seriously threaten the patient's life safety. Attacks in industry and urban infrastructure also show an increasing trend. In the field of automotive embedded systems, more and more electronic devices and embedded devices are used in many high-end automobiles. The attacker can gain control of the car due to the lack of security protection in these devices, such as electronic control unit (ECU) attack [4]. This would have a serious security threat to the driver. Attacks on urban infrastructure can affect the social order, such as attacks on transportation and logistics.

In this paper, we consider the spectrum of challenges, approaches, and practice in IoT security. IoT security is unique in many respects and introduces diverse challenges different from those in security assurance of other computing devices such as desktops, laptops, servers, or even mobile devices [5, 6]. We develop two taxonomies of security attacks specifically for the IoT regime. The first taxonomy introduces attacks on the four-layer architecture of IoT (perception layer, network layer, middleware layer, application layer). Based on this taxonomy, we systematically analyze the security threats and privacy issues on every layer of IoT. The attacks can occur in each layer, and we need to provide protection for the entire IoT structure, not just for the specific technology. Another taxonomy of IoT security and vulnerabilities is based on different application scenarios. This provides an analytical basis for the protection of different IoT applications.

The rest of the paper is organized as follows. Section 2 presents the four-layer architecture of IoT we used to analyze security threats and privacy issues. Section 3 describes the attacks based on IoT architecture, and Section 4 elaborates on a number of attack scenarios. We analyze some challenges in IoT security in Section 5. In Section 6, we analyze the design security framework and security mechanism from the perspective of IoT security requirements. We conclude in Section 7.

2 Generic IoT Architecture

Internet-of-Things architecture can be conveniently viewed as an abstraction of several hierarchical layers. Three key layers in the abstraction are the application layer, the network layer, and the perception layer. The technologies of each layer are different, even though the technology used by the device of the same layer may be heterogeneous. The devices and technology in the Internet-of-Things are used to provide a diversity of services, each with its own requirements, constraints, and trade-offs. Furthermore, the technologies and devices themselves are highly heterogeneous. This makes their management a difficult and complex enterprise. To address this challenge, a middleware layer is also sometimes added to manage different types of service, shielding the underlying implementation details. The task of the middleware layer is to collect information from the network layer and store them into the cloud and database. Besides, the middleware layer also provides data processing ability. The four-layer architecture of the IoT constituted by the above factors is used in this paper, and this architecture can be applied to the actual application development. Figure 1 describes the four-layer architecture of the IoT and the corresponding technologies in each layer. In this section, we discuss the functionality of these layers to motivate their unique security needs.

2.1 Application Layer

The application layer is the social division of the Internet-of-Things, combining with the industry demand and realizing extensive intellectualization [7, 8]. This layer implements different applications for different scenarios. This layer is used to manage and process data from the middleware layer, also providing quality service to the final user [9]. The problem of application layer mainly occurs in the operation of sensitive data, such as illegal access to data, malicious modification of data, and the lifetime of permission [10]. Attackers can exploit code vulnerabilities to attack systems to gain sensitive data and modify it.

2.2 Middleware Layer

The middleware layer obtains data from the network layer, links the system to the cloud and database, and performs data processing and storage [7–10]. With the continuous development of cloud computing and IoT, middleware layer can provide more powerful computing and storage

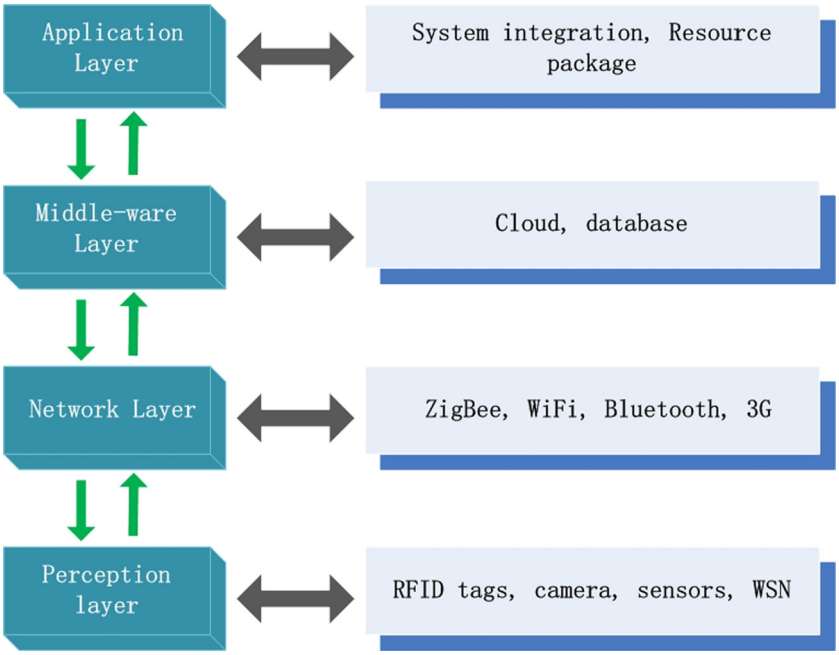

Fig. 1 Four-layer architecture of IoT

capabilities. Meanwhile, this layer provides APIs to meet the demands of the application layer. Database security and cloud security are the main issues in the middleware layer, which affect the quality of service in the application layer.

2.3 Network Layer

This layer is responsible for the connectivity of the IoT infrastrcuture [7–9]. It also collects data from the perception layer and transmits it to the upper layer. The transmission medium can be wired or wireless, and the main technologies are ZigBee, WiFi, Bluetooth, 3G, and so on [11, 12]. Attacks on the network layer are diverse, typically affecting coordination of work and information sharing among devices [10].

2.4 Perception Layer

The perception layer aims at identifying objects and collecting target information, and transforms the information into digital signals [7, 8, 13]. The key technologies of this layer are RFID tags, cameras, sensors, wireless sensor network (WSN), and so on. The technology of perception layer is affected by energy and computing power [9, 14]. At the same time, a sensor device may be working in a hostile environment and can be easily destroyed (intentionally and unintentionally). This has direct effect on the efficiency of the entire system. The main challenge for this layer is the malicious attack on the sensor and identification technology, which interferes with the collection of data [10, 15].

3 IoT Attack Taxonomy Based on Architecture

We now turn to analysis of the IoT attacks and security/privacy issues based on the four-layer architecture described above. Figure 2 presented the attack classification. In this section, we elaborate on the key vulnerability sources and mitigation challenges.

3.1 Application Layer

The attacks in the application layer mainly target (unauthorized) access of sensitive data of the user. Attackers typically exploit the vulnerabilities of programs and application (e.g., code injection, buffer overflow), or unauthorized access to attack. One approach for an unauthorized agent to obtain the same permission as legitimate users is through counterfeiting identity. In addition to these attacks, the application layer is also threatened by viruses, worms, and Trojans. Furthermore, other malicious programs (Rootkit, spyware, adware, etc.) also undermine the privacy of users.

3.1.1 Code Injection

This attack entails introduction of malicious code into the system by exploiting program errors [7, 16]. Code injection can be used for a variety of purposes, e.g., to steal data, get system control, and to propagate worms [10, 17]. The common attacks include shell injection and HTML script injection. This type of attack can cause the system to lose

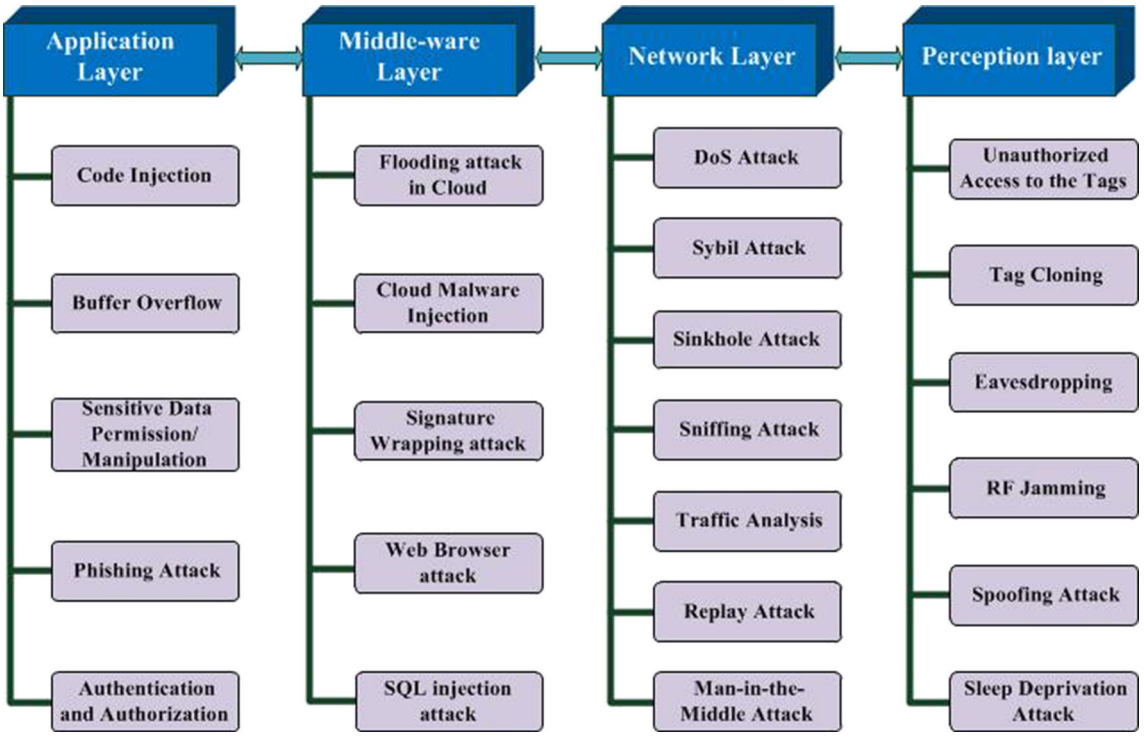

Fig. 2 IoT attacks based on architecture

control and compromise the user's privacy to the attacker, or even to a complete system shutdown.

3.1.2 Buffer Overflow

This attack entails violation of the bounds of code or data buffer by exploiting program vulnerabilities. Many programs work with a pre-defined memory layout for containing code and data segments. The attacker writes a long sequence of data to a specified area, resulting in overflow of the sequence past its pre-defined region of residence. The result can be modification of other data (e.g., when the sequence encroaches the data region of another data buffer), execution of malicious code (e.g., by encroaching into a code segment), and destruction of the program control flow. Common approaches include stack/heap-based buffer overflow, format string attack, integer error, and double free [16, 18, 19]. Buffer overflows represent one of the most common attacks on software and applications. For example, WellinTech KingView 6.53 HistorySvr, an industrial automation software, was threatened by a heap buffer overflow vulnerability [18]. Further, there have been demonstrations showing how this type of attack can enable an unauthorized agent to gain administrator privileges and execute arbitrary code [19].

3.1.3 Sensitive Data Permission/Manipulation

This type of attack refers to illegal access and manipulation of sensitive data, thereby violating user privacy [20–22]. This attack usually exploits design flaws in permission model [23]. There have been demonstrations of attackers exploiting vulnerabilities in the permission model to control applications in smart homes, causing problems such as break-in and theft [20]. Moreover, previous work [21] analyzed the events used to communicate between SmartApp and SmartDevice. Note that SmartApps and SmartDevices represent a particularly vexing problem to data security. A SmartDevice sends sensitive data to SmartApp using events; SmartApp uses events to monitor SmartDevice. However, due to the lack of sufficient protection of the event, this may cause leakage of the event and even cause more serious harm to the user. Additionally, due to the lack of adequate protection for user input, the privacy of users may be violated [23]. In order to solve the above problems, a framework has been proposed to protect sensitive data by declaring intended data flow patterns [22].

3.1.4 Phishing Attack

In this type of exploits, an attacker pretends to be a real user or legitimate institution to obtain sensitive information

about the users, such as passwords and credit card details [7, 24]. The common medium for this attack is email, where sensitive information has been acquired by an attacker when users open the mail.

3.1.5 Authentication and Authorization

Authentication mechanism plays an important role in the protection of IoT security and privacy. The existing authentication mechanisms cannot provide fine-grained verification [19, 25, 26]. For example, apps can download malicious payloads when updated, and attackers can use it to remotely control a device [21, 27]. Meanwhile, there are also vulnerabilities in the permission model. A common problem is over-privilege that permits the device to access information without using all the required [28]. Besides, using the default configuration is also a source of the permission problem. Furthermore, when a file and directory are given inappropriate permission, an attacker may exploit this vulnerability to create attacks in varying degrees [19]. In a specific application scenario considered in previous work, the smart card has vulnerabilities in remote authentication, which may cause user information leakage and tampered [27]. Additionally, because of the lack of a perfect authentication mechanism in the smart home, an attacker can perform unauthorized operations, such as opening the door [21].

3.2 Middleware Layer

The middleware layer provides interfaces and service for the application layer. Attackers can attack the service (e.g., Web service) to affect the application layer. The attack on server and database will affect the information security and operation security of the system. Attacks on the cloud mainly aim at virtualization and data, which poses a huge threat to the privacy of users. The target of the attack on middleware layer is to destroy the quality of service and the privacy of the users.

3.2.1 Flooding Attack in Cloud

This is one form of denial-of-service attacks in the cloud. Here, attackers constantly send requests to a service in the cloud, which depletes the resources in the cloud, thereby affecting the quality of service [29–31]. For sophisticated cloud systems, the side effects of such attacks can be dramatically magnified [30]. When the cloud system finds that the current service instance cannot meet the requirements, it will transfer the affected service to other servers. This will lead to increased work pressure on other servers.

3.2.2 Cloud Malware Injection

The attacker can modify the data, obtain control, and execute malicious code by injecting malicious service instance or virtual machine into the cloud [29–31]. It is mentioned that, for example, attackers copy and upload a victim's service instance, but malicious instance responds to the request when some service requests victim's instance [29]. As a result, the attacker can obtain the sensitive data of service.

3.2.3 Signature Wrapping Attack

Cloud system uses XML signature to ensure the integrity of the service. The attacker modifies the eavesdropped messages without invalidating the signature [29, 30]. It is well known that the Amazon Elastic Cloud Computing (EC2) offers high-quality cloud services [29]. Moreover, EC2 offers SOAP interface to control the deployed machines. Attackers exploit vulnerabilities in SOAP to modify eavesdropped messages. Furthermore, an attacker can execute arbitrary commands and operations as legitimate users.

3.2.4 Web Browser Attack

In the cloud, Web browser is used to execute commands on remote servers, such as authentication and authorization commands [30]. But the browser itself cannot generate encrypted XML tokens. Attackers exploit this weakness to gain access without authentication [24]. The cloud service based on Web service can generate some metadata, which contain a large amount of content related to cloud service and service implementation. Once the attackers obtain these metadata, they may pose a threat to the cloud [30].

3.2.5 SQL Injection Attack

By embedding SQL statements into the input data, a poorly designed program may be vulnerable to such attacks [32, 33]. Attackers use these SQL statements for reading, writing, and deleting operations. This kind of attack can not only obtain the user's private data but also threaten the entire database system. When Web applications are attacked by SQL injection, the current page shows different outcomes compared to the true information [33].

3.3 Network Layer

There are many kinds of networks in IoT, including the Internet and WSN. Different networks use different protocols and devices, so the attacks on the network are also diverse. The most common attack is the DoS attack which

can exhaust network resources and affect the availability of network service. The communication patterns can be obtained by eavesdropping and analyzing the traffic through the network. After obtaining the communication pattern, an obvious attack a malicious agent can perform is the so-called *replay attack*. Besides, there are specific attacks on network node. By compromising a network node, attackers can obtain the transmitted information and gain the control of network, such as Sybil attack, replay attack, and man-in-the-middle attack. The attack in the network layer can also destroy network communication by using the vulnerabilities of network protocols and network nodes.

3.3.1 DoS Attack

In network, a denial-of-service attack (DoS attack) is accomplished by flooding the victim with requests, thereby generating a large amount of network traffic [7, 10, 34, 35]. This type of attack can exhaust all available resources, making network resources unavailable to users. Furthermore, many unencrypted user information can also be leaked [7]. Besides, a distributed denial-of-service attack (DDoS attack) can combine multiple computers as an attack platform and launch DDoS attacks on one or more targets.

3.3.2 Sybil Attack

A node in the system presents multiple identities to the victim node, which allows victim node to execute an operation multiple times, thus defeating redundancy [7, 34, 36]. In wireless sensor network (WSN), since the attacker has multiple identities, victim node may transmit information through compromised node leading to a longer routing distance [34].

3.3.3 Sinkhole Attack

Attackers use comprised node attract data flow from nearby nodes [7, 34, 37]. In [7], the system is fooled and considers the data to have already reached its destination. In a WSN, the attacker may use malicious node to attract the network traffic, and then the sensor data can be operated arbitrarily [34].

3.3.4 Sniffing Attack

Attackers use sniffer devices and applications to obtain network information and then extract valuable data for the further attacks [7, 38].

3.3.5 Traffic Analysis

Attackers deduce the pattern and load of communication, by analyzing the number and the size of the transmitted data packets [35, 38, 39]. The larger the number of packets that can be analyzed, the more valuable information is available. This type of attack can be applied to encrypted packets; its communication pattern can also be analyzed. Three kinds of information can be obtained from WSN through traffic analysis [38]. First, an attacker can detect the activity in the network. Secondly, an attacker can obtain the physical location of wireless access points (APs). Finally, an attacker can learn the information about the protocol type used in the transmission process.

3.3.6 Replay Attack

Attackers obtain information between the two parties by eavesdropping. The received messages are transmitted repeatedly between the communication pairs, thereby exhausting communication resources [16, 40, 41]. In RFID technology, this attack often occurs in the communications between reader and RFID tag. This type of attack not only consumes computing resources between reader and tag, but also consumes the resources of back-end database [40]. In addition to the above effects, attackers can obtain reader grant access by broadcasting radio signal [16].

3.3.7 Man-in-the-Middle Attack

This type of attack is a real-time attack, occurring between two communicating victim nodes. The attacker disguises a node as a legitimate node that communicates with two victim nodes [7, 38, 41, 42]. The attacker gains the trust of two nodes and obtains information about two victim nodes.

3.4 Perception Layer

Perception layer uses a large number of sensor technology and identification technology. Sensor nodes usually use ad hoc network technology to dynamically change the network topology. Sensor nodes often use wireless communication due to the diversity of deployment environment. In this scenario, attackers can easily eavesdrop on communication between nodes. Furthermore, the attacker can directly access the related attributes of the device through physical attacks, and then start further attack, such as tag cloning and spoofing attack. RFID technology is widely used in the perception layer, and attackers can destroy communication between reader and RFID tag, e.g., through RF jamming. The environment of perception layer is relatively restricted by resource and power, so the node uses sleep to prolong life. Attackers can keep the node in working state to accelerate the consumption of the battery, such as sleep deprivation attack. The attack of the perception layer usually aims at destroying the data collection and the communication.

3.4.1 Unauthorized Access to the Tags

RFID systems lack effective authentication techniques, so tags can be easily accessed by unauthorized attackers [7, 38]. Attackers can manipulate data. In wireless sensor networks, once an attacker can access the network, he can launch attack or use the network free of charge.

3.4.2 Tag Cloning

An effective attack involves cloning RFID tags. To do this, the attacker can obtain the relevant information through reverse engineering or directly from its deployment environment [7, 10, 16, 40]. For example, previous work [7] showed compromises where RFID reader cannot tell the difference between original tag and compromised tag.

3.4.3 Eavesdropping

The attackers can easily eavesdrop the device and the node of the perception layer, especially in the wireless communications [7, 16, 40, 41, 43]. In a RFID system, an attacker can use an antenna to record communications between legitimate tags and readers [17, 38, 42]. For example, unauthorized individuals can use the antenna to record data passed between reader and tag [16].

3.4.4 RF Jamming

The attack device sends RF signals to interfere with the communication between the legitimate tag and the readers [7, 16, 40, 44]. An attacker can use RFID tag to interfere with all the signals within its range, thereby preventing reader from communicating with all tags [16]. This type of attack can destroy the data collection process at the perception layer.

3.4.5 Spoofing Attack

Here, the attacker disguises a tag as a valid tag, which gains the same permission and service as the valid tag [16, 34, 40]. Consequently, they can cheat the reader and get the same permissions as the legal tag. In previous work [16], it was shown that in order to obtain the same permission as valid tag, the attacker needs access to the communication channel that is the same as original tag, and must have an in-depth understanding of protocols and authentication. Note that spoofing attacks may lead to packet loss in the transmission process [34]. Furthermore, this type of attack would cause nodes to resend the data, potentially increasing network traffic significantly. It also accelerates the consumption of node power, thus reducing the node lifetime.

3.4.6 Sleep Deprivation Attack

The device and node of the perception layer are limited by the power of the battery. In order to prolong the lifetime, it is necessary for the device to sleep when not working. This type of attack attempts to subvert this process by constantly sending control information to the device and keeping the node in a working state [7, 45].

4 Application Scenarios

Application scenarios for the Internet-of-Things may involve a diversity of domains, including industry, urban infrastructure, smart environment, and healthcare domain (c.f. Fig. 3). The attacks on these scenarios are diverse, cross-cutting across many methods layers in IoT architecture and involving integration and amalgamation of a variety of attack methods. These factors increase the complexity of analyzing IoT security. Additionally, in different application scenarios, the attacker's motivation may be different, e.g., in a wearable application, the target might be access to sensitive user data, while healthcare-related attacks aim at the life safety of patients. The IoT security issues mentioned in this section are complementary to the attack methods introduced in Section 3.

4.1 Industry Domain

4.1.1 Automobile

Today's automobiles are controlled by a number of electronic systems. The trend is expected to grow as the automotive industry moves towards increasingly autonomous vehicles. Unfortunately, while this provides convenience for users and has the potential to improve road safety, it also presents opportunities for some attackers [46, 47]. The automotive systems contain the electronic control units (ECU), the transmission control units, the engine control unit, the telematics unit, the on-board diagnostics (OBD-II) port, and several wireless technologies [4, 48–50], as shown in Fig. 4. Attackers can use relay attacks to attack Passive Keyless Entry and Start (PKES) systems for theft [50]. This type of attack can relay messages between smart key and the car. This attack is independent of authentication, encryption, and protocol. In addition, attackers do not need to be close to smart key to launch attacks. In addition to bypassing the internal network security, attackers can also try to compromise electronic control unit (ECU), telematics unit, brake system, and engine system [48]. Moreover, the attacker can use OBD-II port to inject malicious component into the car's internal network to launch further attacks. Previous work

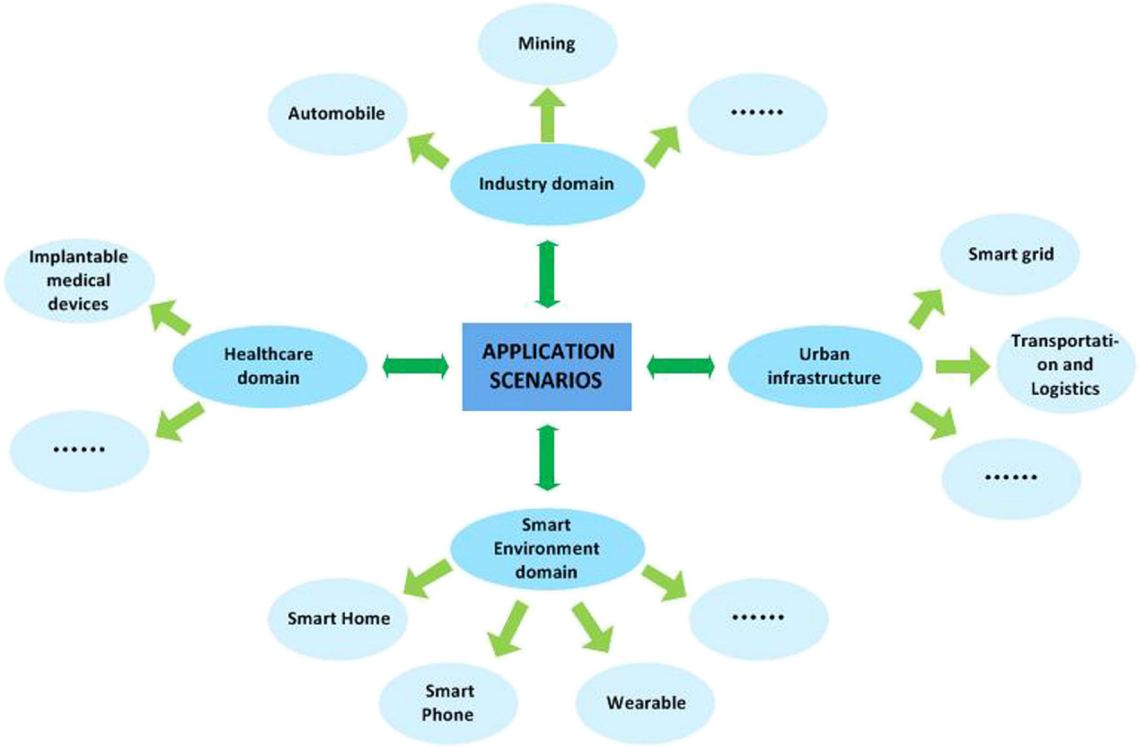

Fig. 3 IoT attacks based on application scenarios

[4] summarizes three attack classifications on the I/O channel: indirect physical access, short-range wireless access, and long-range wireless access. The above attacks will pose a serious threat to the driver's life safety and social order.

4.1.2 Mining

Mine production is often accompanied by dangerous natural disasters such as fire, gas, and floods. Protecting the safety

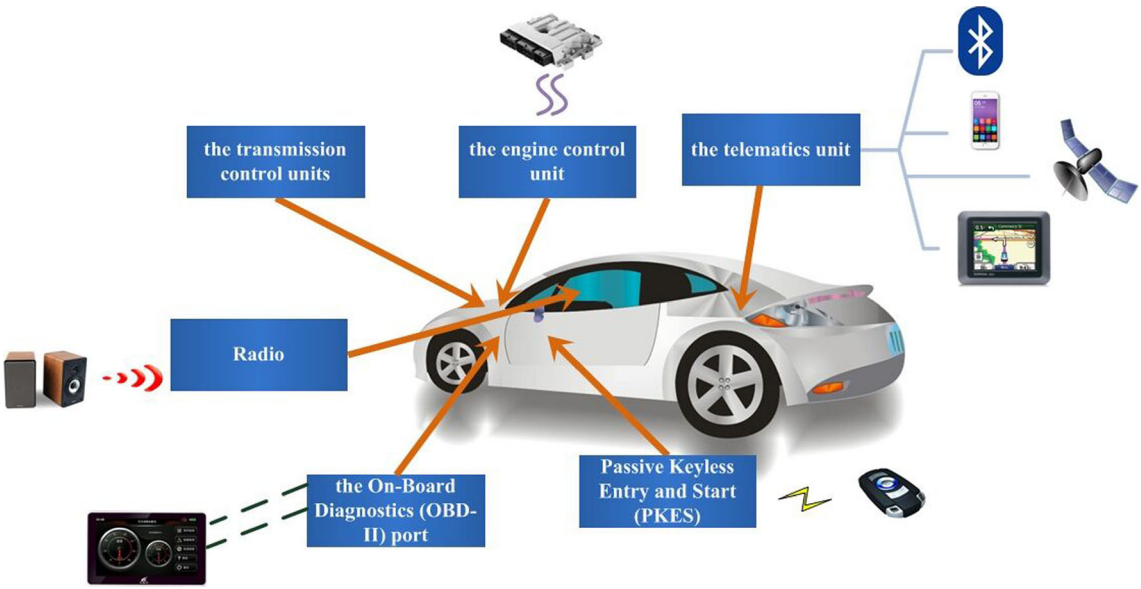

Fig. 4 IoT attacks based on application scenarios

of mine personnel has become a top priority. The application of IoT in mining includes a number of key technologies, such as perception technology, identification technology, WSN technology, and intelligent technology [51]. Using the above technology can effectively detect the occurrence of natural disasters and then advance warning. The IoT-related attacks can also occur in mining areas, which pose a serious threat to the safety of mining personnel.

4.2 Smart Environment Domain

4.2.1 Smart Home

Smart home technology uses home management system to manage home devices and to achieve comfortable, safe home environment. Smart home adopts a series of IoT technology, such as sensor technology, communication technology, and automatic control technology [52, 53], as shown in Fig. 5. Users can communicate directly with home appliances through mobile phones. Smart home technology is targeted to make our life more convenient, save energy, etc. However, it can introduce significant risk to security and privacy. Attackers can directly compromise home devices, thereby undermining the user's security and privacy [54]. In many existing SmartApps, its communication with the device is accomplished by event. Due to the lack of sufficient protection, sensitive information of users can easily be obtained by attackers. Moreover, many of the existing development frameworks of SmartApps have vulnerabilities, and attackers can use these vulnerabilities to achieve a variety of attacks [2, 21].

4.2.2 Smartphone

The combination of mobile terminal and IoT enables consumers to interact with merchants conveniently and obtain information related to goods. Because of the lack of security authentication mechanism and a series of protection mechanisms, the attacker can obtain sensitive data of the user and even attack the mobile phone system and a series of peripheral devices [55].

4.2.3 Wearable

There are many sensor nodes in wearable devices, which are used to collect and transmit information. The information includes sleep patterns, blood pressure, body temperature, heart rate, and ambient environmental information [56]. Wearable devices may contain open program interfaces and test points for multiple purposes [2, 57]. Attackers use them to inject code to obtain the information of user. More seriously, attackers can attack some medical related

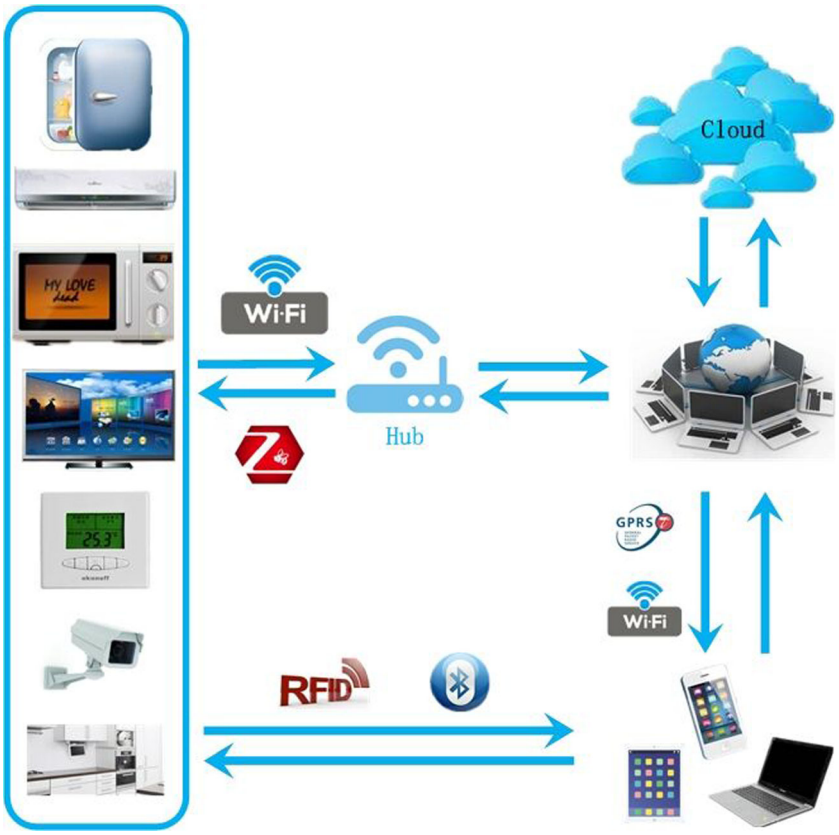

Fig. 5 Architecture of a smart home

wearable devices, thereby threatening the patient's life safety.

4.3 Urban Infrastructure

4.3.1 Smart Grid

Smart grids provide technical support for the grid power generation, transmission, substation, power distribution, and scheduling [58]. They make extensive use of the perception, communication, and data processing capabilities of the IoT. The goal is to promote energy conservation and emission reduction. Smart grids are based on two-way communications and deploy large numbers of embedded devices and sensors to provide intelligent service [59]. Unfortunately, these devices are vulnerable to malicious attacks, which can affect the operation of smart grid and the quality of power grid service. As the interconnectivity of power grids increases, an attacker can collect personal information and violate individual privacy as well.

4.3.2 Transportation and Logistics

With the increasing maturity of Internet-of-Things, its application has recently spread to the fields of transportation and logistics. The continuous development of key technologies of IoT promotes the development of intelligent transportation, which can effectively alleviate the traffic problems, such as traffic congestion and traffic accidents [60]. Intelligent transportation combines IoT technology with traffic management system to monitor and manage traffic. Through the collection of road traffic information and service information, the public can make efficient use of transport facilities. In addition to the above functions, the vehicles can be also perceived and protected. The development of intelligent transportation also promotes the development of other industries, such as intelligent logistics [61]. Intelligent transportation has widely adopted RFID technology, WSN technology, and identification technology, and its security and privacy problems become particularly prominent [54, 62–64]. Intelligent transportation uses sensor technology to obtain traffic emergency information. If an attacker obtains this information, there can be catastrophic consequences.

4.4 Healthcare

The IoT has critical application prospects in the area of health care. This domain can make use of the ability of IoT applications to effectively collect, process, store, transmit, and analyze data [54, 65]. For example, hospitals can share medical data, device data, drug data, personnel data, and management data; RFID technology can be used to identify and locate patients and doctors; and the patient's condition can be monitored and the vital signs can be collected in real time by means of wearable devices. Furthermore, there are implantable medical devices, such as implantable cardioverter defibrillator (ICD). Unfortunately, these devices are also vulnerable to attack due to the lack of effective security mechanisms. Attackers can use software radio-based attacks to threat ICD devices, which will pose a great threat to the patient's life [3, 66]. At the same time, the attacker can use RFID vulnerabilities to obtain patient privacy information.

5 Challenges of Internet-of-Things Security

We now turn to some unique challenges to IoT security. We consider challenges from three aspects: unreliable communication, hostile environment, and inadequate data and privilege protection.

5.1 Unreliable Communication

Because of the diversity communication media used in propagating potentially sensitive data, IoT applications can be vulnerability to a number of security vulnerabilities. Each such vulnerability can be unique, based on the medium involved. Wireless medium is one of the most vulnerable candidates. Note that the nature of this medium is broadcasting. Consequently, the transmission process based on this kind of media is vulnerable to eavesdropping, replay attack, and tampering attacks. The attacker can also inject malicious code into the wireless routing node, thereby affecting the communication of the whole wireless network. Collision is also a problem in wireless networks: even if channel is available, it cannot guarantee that the communication is reliable. Another critical problem is delay, particularly for applications that impose real-time constraints. In complex environments, there is large-scale deployment of sensor nodes via several ad hoc technologies, making manageability a non-trivial issue. Finally, the network topology is vulnerable to environment and node failure, which can compromise the reliability of information transmission.

5.2 Hostile Environment

In IoT applications, many devices and nodes are deployed in a hostile environment, i.e., within physical vicinity of the attacker. Attackers can consequently obtain information about devices and nodes through physical access, which can enable attacks such as tag cloning and, even worse, can physically destroy the device directly. At the same time, in the hostile environment, the energy consumption of

device also has certain requirements, making the device is resource-constrained. Attackers can exploit these constraint sto launch a series of attacks, such as sleep deprivation attack. Furthermore, resource constraints often preclude application of sophisticated security framework and security algorithms on such devices.

5.3 Inadequate Data and Privilege Protection

The issues of data security and permission have clear correspondence with Internet-of-Things security. Because of the lack of permission protection, the attacker can remotely access and modify the data in the system. The vulnerabilities with authorization, such as the over-privilege, can allow attackers to perform unauthorized operations. Users' privacy is often easily violated due to the lack of protection for user input. In addition, by exploiting bugs on the program, attackers can inject malicious code into the system and extract data.

6 Designing for Security: Challenges and Approaches

In this section, we turn to an analysis of IoT security assurance from the point of view of system design. First, we analyze several requirements that must be met and some countermeasures. Some key requirements are shown in Table 1. Here, we elaborate on these requirements.

Table 1 IoT security requirements

Quality attribute	IoT security description
Data integrity	Data integrity ensures data integrity, reliability, and correctness and confirms that data has not been modified and destroyed.
Data confidentiality	Data confidentiality aims at concealing data from unauthorized individuals, thus protecting users' privacy and sensitive data without being acquired by attackers. Only legitimate users can access the information.
Data availability	Data availability is used to make sure that resources (e.g., data and service) are available.
Authentication	Authentication defines verification and differentiation of identities that can access entities. In IoT, authentication protocols play an important role in the mutual communication among different entities.
Authorization	Authorization defines the process of granting, denying, and restricting access to entities. The authorization scheme performs different operations according to different entities.

6.1 Data Integrity

Data is easily captured and modified and can cause servers to crash in the transmission process. Malicious nodes can inject erroneous information into the network. At the same time, hostile communication environment can also cause loss of data. Checksum and cyclic redundancy check (CRC) are usually used to detect or verify errors that may occur after data transmission or storage. In addition, message authentication code (MAC), digital signature, and version control are also used to ensure the integrity of data.

6.2 Data Confidentiality

There are many ways to ensure data confidentiality. The commonly used methods include access control and data encryption. Data encryption is the process of converting data to ciphertext such that the original content (called *plaintext*) cannot be accessed until a certain authorization (e.g., decryption key) is obtained. Commonly used encryption algorithms are RSA, DSA, AES, etc. In addition, access control is also a feasible method to control access to system resources by identifying visitors' identities. However, due to the limited resources in IoT devices or embedded devices, sophisticated data encryption and authentication scheme cannot be fully applied, so it cannot provide sufficient protection.

6.3 Data Availability

The availability of information resources is critical to users, and this is an important step in ensuring the quality of service (QoS). The goal of denial of service (DoS) attack is to make the resources unavailable to users. An effective way to ensure data availability is to provide multiple paths for data transmission, thereby enhancing the ability of attack detection. When a path is not available, other paths can also provide service to ensure the QoS.

6.4 Authentication and Authorization

Authentication and authorization constitute critical first defense against intrusion. Attackers often exploit the vulnerabilities in authentication and authorization to access the system. For example, in SmartApp, the attacker can violate the privacy of the user because of the lack of effective protection for user input. In addition, in smart home, attackers can bypass authentication and authorization mechanisms and can execute malicious operation on intelligent devices in the home. The most common way to solve these problems is to adopt a systematic access control paradigm, such as role-based access control (RBAC). An entity can play multiple roles and each role has different

functions. The system manages access and permission according to the role.

There are several ways to launch an attack in a specific application scenario. For example, the attacks on the SCADA system can be launched from the software level and the hardware level. An attacker can physically access the system to modify the data, and even if the emergency has occurred, it will not trigger the actual alarm mechanism. Moreover, an attacker can modify the display value to delay human response to an emergency. From the software level, attackers can also exploit program vulnerabilities, such as buffer overflow, SQL injection, and other attack methods to destroy the system. In addition, the attacker can also use the vulnerabilities in communication protocol. Because SCADA has real-time requirements for information processing, attackers can delay important data in emergency situations by using flood attack, which may lead to an uncertain disaster. Therefore, in the design of security mechanisms and security framework, we must consider not only specific attack methods but also the integration of a variety of attack methods, from a more comprehensive perspective to deal with IoT security issues.

7 Conclusion

The IoT technology has changed people's life style due to information collection, communication, and processing abilities. In the development of the Internet-of-Things, one of the major obstacles is security and privacy issues. IoT attacks may cause privacy violation and threaten people's life and privacy safety. Protecting the privacy of users has become another important challenge in the development of IoT. Many researches focus on IoT security and privacy, but the countermeasures presented in these research often aim at a particular type of attack. Therefore, it is necessary to consider the IoT architecture as a whole and provide holistic protections.

In this paper, we discuss the security threats and privacy concerns in each layer of the IoT architecture. We discussed two attack classifications, one based on the IoT architecture and another based on application scenarios. The attack in IoT is analyzed according to different classification standards. The security of each layer on the IoT architecture should be implemented at the same time. Significant further research is required to design a comprehensive security mechanism for the entire IoT architecture.

Acknowledgements This paper is partially supported by the National Key Research and Development Program of China under grant no. 2016YFC0801607, the National Natural Science Foundation of China (NSFC) under grant no. 61602104, the National Science Foundation (DGE-1802701, CNS-1739736), and Cisco.

References

1. Iqbal MA, Olaleye OG, Bayoumi MA (2017) A review on Internet of Things (IoT): security and privacy requirements and the solution approaches, Global Journal of Computer Science and Technology
2. Arias O, Ly K, Jin Y (2017) Security and privacy in IoT era. In: Smart Sensors at the IoT Frontier. Springer, pp 351–378
3. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, Fu K, Kohno T, Maisel WH (2008) Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. In: IEEE Symposium on Security and Privacy, 2008. SP 2008. IEEE, pp 129–142
4. Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S, Koscher K, Czeskis A, Roesner F, Kohno T et al (2011) Comprehensive experimental analyses of automotive attack surfaces. In: USENIX Security Symposium San Francisco
5. Ray S, Peeters E, Tehranipoor M, Bhunia S (2017) System-on-chip platform security assurance: architecture and validation. In: Proceedings of the IEEE
6. Ray S (2017) System-on-chip security assurance for IoT devices: cooperations and conflicts. In: IEEE Custom Integrated Circuitsx Conference
7. Farooq MU, Waseem M, Khairi A, Mazhar S (2015) A critical analysis on the security concerns of Internet of Things (IoT). Int J Comput Appl 111:7
8. Khan R, Khan S, Zaheer R, Khan S (2012) Future internet: the Internet of Things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology (FIT). IEEE, pp 257–260
9. Wu M, Lu T-J, Ling F-Y, Sun J, Du H-Y (2010) Research on the architecture of Internet of Things. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol 5. IEEE, pp V5–484
10. Zhang W, Qu B (2013) Security architecture of the Internet of Things oriented to perceptual layer. Int J Comput, Consum Control (IJ3C) 2(2):37–45
11. Cui A, Stolfo SJ (2010) A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan. In: Proceedings of the 26th Annual Computer Security Applications Conference. ACM, pp 97–106
12. Mattern F, Floerkemeier C (2010) From the internet of computers to the Internet of Things, From active data management to event-based systems and more, pp 242–259
13. Jia X, Feng Q, Fan T, Lei Q (2012) RFID technology and its applications in Internet of Things (IoT). In: 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet). IEEE, pp 1282–1285
14. Li L (2012) Study on security architecture in the Internet of Things. In: 2012 International Conference on Measurement, Information and Control (MIC), vol 1. IEEE, pp 374–377
15. Pateriya R, Sharma S (2011) The evolution of RFID security and privacy: a research survey. In: 2011 International Conference on Communication Systems and Network Technologies (CSNT). IEEE, pp 115–119
16. Mitrokotsa A, Rieback MR, Tanenbaum AS (2010) Classification of RFID attacks. Gen 15693:14443
17. Yampolskiy M, Horvath P, Koutsoukos XD, Xue Y, Sztipanovits J (2013) Taxonomy for description of cross-domain attacks on CPS. In: Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems. ACM, pp 135–142
18. Zhu B, Joseph A, Sastry S (2011) A taxonomy of cyber attacks on SCADA systems. In: Internet of Things (Ithings/CPSCom), 2011 international conference on and 4th international conference on Cyber, Physical and Social Computing. IEEE, pp 380–388

19. Simmons C, Ellis C, Shiva S, Dasgupta D, Wu Q (2009) AVOIDIT: a cyber attack taxonomy
20. Jia YJ, Chen QA, Wang S, Rahmati A, Fernandes E, Mao ZM, Prakash A, Unviersity SJ (2017) ContexIoT: towards providing contextual integrity to appified IoT platforms. In: Proceedings of the 21st Network and Distributed System Security Symposium (NDSS'17)
21. Fernandes E, Jung J, Prakash A (2016) Security analysis of emerging smart home applications. In: 2016 IEEE Symposium on Security and Privacy (SP). IEEE, pp 636–654
22. Fernandes E, Paupore J, Rahmati A, Simionato D, Conti M, Prakash A (2016). In: USENIX Security Symposium, pp 531–548
23. Nan Y, Yang M, Yang Z, Zhou S, Gu G, Wang X (2015) UIPicker: user-input privacy identification in mobile applications. In: USENIX Security Symposium, pp 993–1008
24. Thakur BS, Chaudhary S (2013) Content sniffing attack detection in client and server side: a survey. Int J Advan Comput Res 3(2):7
25. Alqassem I, Svetinovic D (2014) A taxonomy of security and privacy requirements for the Internet of Things (IoT). In: 2014 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). IEEE, pp 1244–1248
26. Babar S, Mahalle P, Stango A, Prasad N, Prasad R (2010) Proposed security model and threat taxonomy for the Internet of Things (IoT). In: 2010 Recent Trends in Network Security and Applications, pp 420–429
27. Chang C-C, Hwang K-F (2003) Some forgery attacks on a remote user authentication scheme using smart cards. Informatica 14(3):289–294
28. Bugiel S, Heuser S, Sadeghi A-R (2013) Flexible and fine-grained mandatory access control on Android for diverse security and privacy policies. In: USENIX Security Symposium, pp 131–146
29. Gruschka N, Jensen M (2010) Attack surfaces: a taxonomy for attacks on cloud services. In: 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD). IEEE, pp 276–279
30. Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On technical security issues in cloud computing. In: 2009 IEEE International Conference on Cloud Computing. CLOUD'09. IEEE, pp 109–116
31. Padhy RP, Patra MR, Satapathy SC (2011) Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS) 1(2):136–146
32. Zhang Q, Wang X (2009) SQL injections through back-end of RFID system. In: 2009 International Symposium on Computer Network and Multimedia Technology. CNMT 2009. IEEE, pp 1–4
33. Dorai R, Kannan V (2011) SQL injection—database attack revolution and prevention. J Int'l Com L & Tech 6:224
34. Sastry AS, Sulthana S, Vagdevi S (2013) Security threats in wireless sensor networks in each layer. Int J Advan Netw Appl 4(4):1657
35. Babar S, Stango A, Prasad N, Sen J, Prasad R (2011) Proposed embedded security framework for Internet of Things (IoT). In: 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE). IEEE, pp 1–5
36. Douceur JR (2002) The Sybil attack. In: International Workshop on Peer-to-Peer Systems. Springer, pp 251–260
37. Ahmed N, Kanhere SS, Jha S (2005) The holes problem in wireless sensor networks: a survey. ACM SIGMOBILE Mobile Comput Commun Rev 9(2):4–18
38. Welch D, Lathrop S (2003) Wireless security threat taxonomy. In: 2003 IEEE Systems, Man and Cybernetics Society and Information Assurance Workshop. IEEE, pp 76–83
39. Padmavathi DG, Shanmugapriya M et al (2009) A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv:0909.0576
40. Ding Z-h, Li J-t, Feng B (2008) A taxonomy model of RFID security threats. In: 2008 11th IEEE International Conference on Communication Technology. ICCT 2008. IEEE, pp 765–768
41. Cho J-S, Yeo S-S, Kim SK (2011) Securing against brute-force attack: a hash-based RFID mutual authentication protocol using a secret value. Comput Commun 34(3):391–397
42. Hossain MM, Fotouhi M, Hasan R (2015) Towards an analysis of security issues, challenges, and open problems in the Internet of Things. In: 2015 IEEE World Congress on Services (SERVICES). IEEE, pp 21–28
43. Papp D, Ma Z, Buttyan L (2015) Embedded systems security: threats, vulnerabilities, and attack taxonomy. In: 2015 13th Annual Conference on Privacy, Security and Trust (PST). IEEE, pp 145–152
44. Khoo B (2011) RFID as an enabler of the Internet of Things: issues of security and privacy. In: 2011 International Conference on Internet of Things (ithings/CPSCom) and 4th International Conference on Cyber, Physical and Social Computing. IEEE, pp 709–712
45. Bhattasali T, Chaki R, Sanyal S (2012) Sleep deprivation attack detection in wireless sensor network. arXiv:1203.0231
46. Da Xu L, He W, Li S (2014) Internet of Things in industries: a survey. IEEE Trans Ind Inf 10(4):2233–2243
47. Ray S, Chen W, Bhadra J, Al Faruque MA (2017) Extensibility in automotive security: current practice and challenges. In: Proceedings of the 54nd Annual Design Automation Conference
48. Koscher K, Czeskis A, Roesner F, Patel S, Kohno T, Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H et al (2010) Experimental security analysis of a modern automobile. In: 2010 IEEE Symposium on Security and Privacy (SP). IEEE, pp 447–462
49. Qin E, Long Y, Zhang C, Huang L (2013) Cloud computing and the Internet of Things: technology innovation in automobile service. In: International Conference on Human Interface and the Management of Information. Springer, pp 173–180
50. Francillon A, Danev B, Capkun S (2011) Relay attacks on Passive Keyless Entry and Start Systems in modern cars. In: Proceedings of the 18th Annual Network and Distributed System Security Symposium. The Internet Society. Citeseer
51. Qiuping W, Shunbing Z, Chunquan D (2011) Study on key technologies of Internet of Things perceiving mine. Procedia Eng 26:2326–2333
52. Hernandez G, Arias O, Buentello D, Jin Y (2014) Smart Nest thermostat: a smart spy in your home, Black Hat USA
53. Ling Z, Liu K, Xu Y, Jin Y, Fu X An end-to-end view of IoT security and privacy
54. Kumar JS, Patel DR (2014) A survey on Internet of Things: security and privacy issues. Int J Comput Appl 90:11
55. Bai X, Xing L, Zhang N, Wang X, Liao X, Li T, Hu S-M (2016) Staying secure and unprepared: understanding and mitigating the security risks of Apple ZeroConf. In: 2016 IEEE Symposium on Security and Privacy (SP). IEEE, pp 655–674
56. Arias O, Wurm J, Hoang K, Jin Y (2015) Privacy and security in Internet of Things and wearable devices. IEEE Trans Multi-Scale Comput Syst 1(2):99–109
57. Ray S, Yang J, Basak A, Bhunia S (2015) Correctness and security at odds: post-silicon validation of modern SoC designs. In: Proceedings of the 52nd Annual Design Automation Conference
58. Liu J, Xiao Y, Li S, Liang W, Chen CP (2012) Cyber security and privacy issues in smart grids. IEEE Commun Surv Tutorials 14(4):981–997
59. Shepard DP, Bhatti JA, Humphreys TE, Fansler AA (2012) Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. In: Proceedings of the ION GNSS Meeting, vol 3, pp 3591–3605

60. Zhou H, Liu B, Wang D (2012) Design and research of urban intelligent transportation system based on the Internet of Things. Internet of Things, pp 572–580
61. Zhang Y, Chen B, Lu X (2011) Intelligent monitoring system on refrigerator trucks based on the Internet of Things. In: International Conference on Wireless Communications and Applications. Springer, pp 201–206
62. Gill S, Sahni P, Chawla P, Kaur S (2017) Intelligent transportation architecture for enhanced security and integrity in vehicles integrated Internet of Things. Indian J Sci Technol 10:10
63. Tyagi P, Dembla D (2014) Investigating the security threats in Vehicular ad hoc Networks (VANETs): towards security engineering for safer on-road transportation. In: ICACCI 2014 International Conference on Advances in Computing, Communications and Informatics. IEEE, pp 2084–2090
64. Ray S (2017) Transportation security in the era of autonomous vehicles: challenges and practice. In: Proceedings of International Conference on Computer-Aided Design
65. Atzori L, Iera A, Morabito G (2010) The Internet of Things: a survey. Comput Netw 54(15):2787–2805
66. Hanna S, Rolles R, Molina-Markham A, Poosankam P, Blocki J, Fu K, Song D (2011) Take two software updates and see me in the morning: the case for software security evaluations of medical devices in HealthSec