Digital Communications and Networks xxx (xxxx) xxx

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Security and privacy issues of physical objects in the IoT: Challenges and opportunities

Xuanxia Yao [a], Fadi Farha [a], Rongyang Li [a], Ismini Psychoula [b], Liming Chen [b], Huansheng Ning [a,*]

[a] School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, 100083, China
[b] School of Computer Science and Informatics, De Montfort University, Leicester, UK

ARTICLE INFO

Keywords:
Security
Privacy preserving
Physical objects
Life cycle
Internet of things

ABSTRACT

In the Internet of Things (IoT), security and privacy issues of physical objects are crucial to the related applications. In order to clarify the complicated security and privacy issues, the life cycle of a physical object is divided into three stages of pre-working, in-working, and post-working. On this basis, a physical object-based security architecture for the IoT is put forward. According to the security architecture, security and privacy requirements and related protecting technologies for physical objects in different working stages are analyzed in detail. Considering the development of IoT technologies, potential security and privacy challenges that IoT objects may face in the pervasive computing environment are summarized. At the same time, possible directions for dealing with these challenges are also pointed out.

1. Introduction

The basic function of the Internet of Things (IoT) system is to collect data from the physical world and provide services for users according to their requests or the results of data processing. Cyber entities in the IoT are always mapped to physical objects that have the ability to interact with each other [1]. They collaborate to complete specific tasks. As an application-driven network, the IoT has been applied not only in academic research or industrial field, but also in daily life, such as smart grid, e-health, e-home, environment monitoring, smart city, and so on [2]. Furthermore, cross-application or cross-domain IoTs [3,4] are very common now. Since these IoT-based applications are always related to daily life or work, more and more people begin to concern privacy [5], and at the same time, the security problems become more and more complicated.

Physical objects as the core of the IoT, and their security and privacy are crucial to IoTs and their applications. Physical objects in the IoT have six distinctive features [1]: spatiotemporal inconsistency, multi-identity coexistence, high heterogeneity, resource-constraint, dynamics, and social awareness, making their security and privacy issues very complicated, and the traditional security and privacy-preserving mechanisms are unsuitable or ineffective for them. Most of existing security architectures only focus on the security issues in the perception layer, network layer, and application layer [6,7]. They cannot fully describe the security and privacy issues of the IoT. Huansheng Ning et al. put forward a security architecture for their Unit and Ubiquitous IoT (U2IoT) [8], which extends the traditional IoT security architecture. Since it is modeled from the aspects of information security in the cyber world, physical security in the physical world, and management security in human society, it comprehensively covers the security issues of U2IoT. However, the cyber-physical-social security architecture is designed for U2IoT and not universal to the IoT-based pervasive computing environment. In addition, the privacy issue is not considered enough.

To address these problems, we try to divide the life cycle of the IoT physical object into three stages of pre-working, in-working, and post-working according to their working status. On this basis, we construct a security architecture based on physical objects in order to analyze the security and privacy issues in the three stages respectively.

2. The physical object-based security architecture for IoT

The physical object-based security architecture for the IoT is constructed according to the objects' status and the IoT's architecture, as shown in Fig. 1. It can be seen that physical objects in different stages have different characteristics, security and privacy problems. For clarity, physical objects are analyzed from the three stages respectively.

* Corresponding author.
E-mail address: ninghuansheng@ustb.edu.cn (H. Ning).

https://doi.org/10.1016/j.dcan.2020.09.001
Received 12 September 2019; Received in revised form 26 August 2020; Accepted 1 September 2020
Available online xxxx

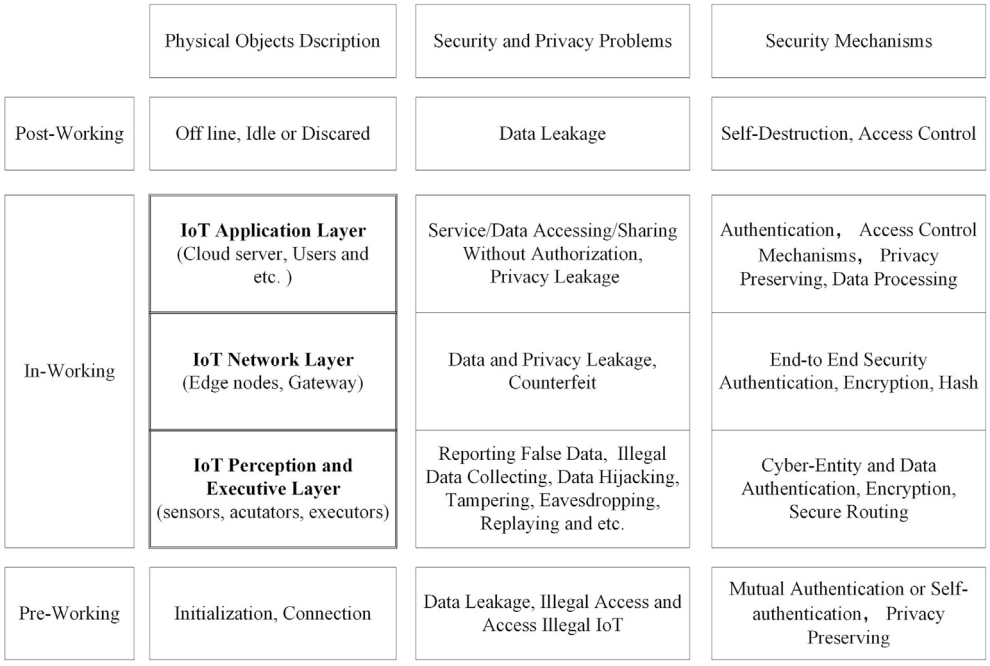

Fig. 1. The physical object-based security architecture for the Internet of Things.

2.1. Physical objects in pre-working

The physical object in pre-working is the entity ready to access the IoT, and its status is essentially the process of mapping the entity in the physical world to a cyber object in the IoT. The mapping process includes two phases of initialization and connection.

In the initialization phase, the required data, parameters and functions are preloaded to the physical object, which is usually done by its owner or the legal operator in the secure environment. And the physical object is inactive at this time, its security and privacy-preserving requirements can be met by physical tools, social means and management measures.

In the connection phase, the physical object becomes active and tries to connect to the specific IoT. As a stranger, it may be denied accessing the legal IoT or be connected to an unintended, illegal or malicious IoT. The former will inevitably lead to access failure, and the latter may lead to data leakage or being attacked. To avoid these security and privacy problems, both the physical object and the IoT need to perform the appropriate security mechanisms. For the physical object to be an IoT node, the premise of its security and privacy-preserving is to check whether the IoT is the one that it is expected to access. It is usually achieved by authenticating the physical object or specific node in the IoT. And for the IoT, it is a prerequisite to verify the legitimacy of the strange physical object so as to avoid the illegal or malicious node joining it. It is usually done by the IoT's nodes within the stranger's communication range and requires the strange connector to provide some identity data, which may cause privacy breach. In summary, mutual authentication with privacy-preserving is a common way to realize a secure connection.

2.2. Physical objects in in-working

It can be seen from Fig. 1 that physical objects in in-working span the three layers of the IoT's architecture. In each layer, there are different tasks, security, and privacy problems.

2.2.1. Physical objects in the perception and executive layer

Most of the physical objects in the perception and executive layer are various nodes with the ability of sensing. And some objects also have the ability to execute the instructions. They usually have limited resources and are deployed in unattended locations. These nodes are not only responsible for data sensing, collecting, aggregating, but also involved in data using and sharing, and even the execution of commands. Since data is the foundation of IoT-based applications, the security of data is of paramount importance, which largely depends on the security of physical objects.

The common attacks on physical objects in the perception and executive layer mainly include the attacks on the physical nodes themselves and the sensed data. The former usually includes physical destruction, battery draining, illegal reading, and writing, etc., which are generally launched by the attacker close to the physical target object and with the purpose of destroying, disabling the physical object, stealing or falsifying its configuration. In order to resist these attacks, it is necessary to enhance the security of the physical object in its designing phase and provide indispensable security measures in physical objects. Attacks on the sensed data are usually launched during data collecting, transmitting, and using, such as forging, hijacking, tampering, eavesdropping and replaying the sensed data. They may cause data disclosure, loss, abuse or malicious use, out of date or spatiotemporal inconsistency, etc., and further harm the attacked physical object itself and its owner or user. In order to prevent these attacks and secure the sensed data, encryption, authentication, hash and secure routing mechanism are often used.

2.2.2. Physical objects in the networking layer

The networking layer is a dynamic and heterogeneous communication infrastructure formed by connecting various access networks (such as WiFi, WiMax, 4G, 5G, etc.) to the Internet. It is responsible for transmitting the data acquired from the perception layer to the data or control center. Physical objects in the networking layer are usually edge nodes in the IoT, which act as the gateway. Since IP-based communication is the main communication mode, all the security and privacy vulnerabilities in the IP networks are in front of physical objects in the networking layer. At the same time, various connection, security and privacy requirements of physical objects in the perception and executive layers have to be met. In practice, these physical objects are also heterogeneous and dynamical. Furthermore, they are usually resource-constraint in most cases. To deal with these security and privacy problems, lightweight authentication, encryption and privacy-preserving mechanisms are necessary.

2.2.3. Physical objects in the application layer

Physical objects in the application layer are usually IoT users and actuators or executors. IoT users usually aim to obtain data or services from the system, and actuators/executors are usually responsible for receiving instructions from the system and performing the specified task.

Nowadays, IoT covers a wide range of applications, from smart homes (e.g., smart light, smart home appliances), smart healthcare (e.g., telemedicine, real-time health monitoring) to smart industries (e.g., digital manufacturing, environmental monitoring) and smart cities (e.g., smart traffic, smart parking), etc. All of them are data-driven [9]. Since data always changes with applications, the security and privacy issues of physical objects in the application layer are very complicated.

For one thing, different applications have different requirements for data and privacy and face different security issues. For instance, in smart health, the data is closely related to the user's privacy, and its accuracy and correctness are crucial to the user's life. While in the smart city, data is usually from crowdsensing, most of the data is insensitive, and the accuracy requirement is not as strict as in smart health.

For another, the application layer is also the data sharing and processing platform for multiple applications, and secure data sharing and processing are very important. Furthermore, the data in the application layer is always directly or indirectly associated with the physical object's user or owner, so data processing and sharing have to face the challenge of privacy leakage.

In order to protect the security and privacy of the physical objects involved in the application layer, authentication, access control and secure data processing methods with privacy-preserving are always indispensable.

2.3. Physical objects in post-working

Physical objects in post-working are usually offline, idle or even discarded nodes. They are vulnerable to being compromised by an attacker. Since the data in these physical objects may be related to the security and/or the privacy of the IoT and the users, they are always targets of attack. The data leakage of physical objects in post-working not only threatens the security of the IoT, but also makes the physical objects in in-working vulnerable to being attacked, compromised, and privacy leakage.

To deal with the security and privacy problems of physical objects in post-working, lightweight authentication and access control are prerequisites. In addition, some physical protection measures or self-destruction mechanisms are also very effective. Physical protection measures make the illegal reading and writing very hard or infeasible. And the self-destruction mechanism will be triggered when an unauthorized operation occurs, which makes physical objects and/or the data in them unusable. However, these two mechanisms are often difficult or costly to implement.

3. Security and privacy issues of physical objects in pre-working

In the initialization state, physical objects are usually pre-loaded with some security parameters and/or work in a security and trusted environment, so the security and privacy-preserving requirements can be guaranteed. In the connection state, a physical object tries to access an existing IoT or connect with other physical objects. Since both sides do not know each other in advance, there are many security and privacy problems, such as data leakage, illegal accessing and connecting to a malicious IoT, etc. In this section, we firstly analyze security and privacy requirements of IoT physical objects in the connection status. And then, we make a survey on the existing security and privacy-preserving technologies for them.

3.1. Security and privacy requirements for physical objects in connection state

The security and privacy requirements for physical objects in connection state are usually closely related to the mode of their accessing or connecting to the IoT. In general, the IoT objects' connection modes can be roughly classified into two kinds according to the number of the physical objects accessing the same point of the IoT simultaneously, which are single access mode and bulk access mode.

3.1.1. Characteristics of the single access mode

Single access mode means that each physical object is individually connected the IoT. According to the IoT application environment, there are two situations.

In Unit IoT applications [1], physical objects are usually required to be registered or pre-deployed in the initialization state. Since the connection is in the host domain, the security and privacy issues are relatively simple. For the visited IoT, checking the registration information of a physical object is a basic method to prevent illegal node access. For the object that has access to the IoT in the single access mode, keeping its registration information confidential is crucial to anti-counterfeiting, and identifying the authenticity or legitimacy of the IoT is a prerequisite to avoid connecting to an unfamiliar, malicious IoT or cyber-entity.

In ubiquitous IoT applications [1], physical objects usually need to connect to different domains, and the security and privacy problems are much complicated. For one thing, the identity, role, and attributes of the physical objects always change with time and space, which requires a flexible connection admission mechanism so as to make them to access the IoT ubiquitously. For another, there is no trust relationship between the visiting physical object and the visited domain, both of them need to avoid establishing a connection with an illegal or malicious one. Meanwhile, the sensitive data of the physical object should not be revealed to any strange entity.

3.1.2. Characteristics of the bulk access mode

The bulk access is generally a many-to-one or many-to-many connection mode for the purpose of high efficiency, which usually occurs in RFID systems, Vehicle-to-Grid (V2G) environments, and vehicular networks. They are characterized by large-scale, concurrent access, sporadic or intermittent connections, limited communication range, and so on. And the physical objects' security and privacy requirements often vary with the environment.

In the RFID system, an RFID tag is used as the identifier of the physical object, and it is always the target of attack. Essentially, RFID-based IoT applications are designed to identify or track physical objects, such as anti-counterfeiting, supply chain management, and mobile tracking [10]. The secure connection between the tag and the reader is the basis for the security of the RFID system, as well as the basis for the protection of physical objects. For instance, attackers may try to use an illegal reader to read data from legitimate tags, which may lead to physical objects' privacy leakage. And at the same time, attackers can also forge a tag to deceive customers into thinking that the fake productions or physical objects are authentic. In addition, attackers can eavesdrop on the data exchanged between the RFID tag and the reader. It is obvious that the authenticity of the tag and reader are crucial to the security of an RFID system. Meanwhile, the confidentiality of the data in the tag and the data exchanged between the tag and the reader is very important to the physical objects' privacy.

In the V2G environment, it is very common for multiple electric vehicles to communicate with an aggregator in the smart grid simultaneously. Similarly, a roadside unit in the vehicular ad hoc network

always receives multiple vehicle requests at the same time. Since vehicle data is closely related to vehicle owners or users, and involves the personal safety and the economic interests of them and the smart grid providers, the legitimacy, authenticity of the vehicles, roadside unit, and aggregator are very important to V2G and Vehicular Ad-hoc Networks (VANET). Furthermore, the exchanged data, especially the sensitive data, always needs to be kept secret to avoid privacy leakage. Consequently, the connection or interaction between the vehicle and the access point (such as the aggregator in V2G, and the roadside unit in VANET) should be authenticated through privacy-preserving.

3.1.3. Security and privacy requirements analysis

Although the connection modes varying with the application environments may lead to changes in security and privacy requirements accordingly, any connection mode (one-to-one, many-to-one, and many-to-many) always involves two parts of the initiator and the receiver. If an illegal object succeeds in launching a connection (as a connection initiator) or defrauding the connection initiator (as a connection target), the sensitive data may leak, and the related physical objects may suffer some loss. In order to avoid connecting with dishonest or malicious objects and leaking privacy, the security and privacy requirements of physical objects in connection state can be summarized as the following two aspects.

Illegal or malicious object detection: In the single connection mode, the connection initiator may be a physical object trying to get the service from the IoT or an IoT object trying to collect data from the sensors, etc. In the bulk access mode, the connection initiator may be an IoT access point (such as an RFID reader, a roadside unit or an aggregator, etc.) or a generic physical object trying (such as an RFID tag, an intelligent vehicle, and so on) to connect the access point. In practice, the connection initiator and the connection target always vary with the application and environment. For instance, in most RFID systems, the reader is usually the connection initiator, and the RFID tag is always the connection target. And in V2G or VANET, vehicles, the roadside unit and the aggregator may be either the initiator or the target. Since both the connection initiator or the connection target (the connected physical object) may be illegal in the connection process, the illegal or malicious object detection includes identifying and distinguishing all physical objects involved in the connection process.

Privacy preserving: Similarly, the privacy requirements usually vary with environments too. In the ubiquitous IoT, the physical objects launching a cross-domain access always need to keep its sensitive data secret from the visited domain. In most RFID-based applications, such as anti-counterfeiting [10,11], the data in an RFID tag is always confidential, which represents the identity, state or attributes of the physical object attached to it. The leakage of RFID data is equivalent to breaching the object's privacy and will lead to forgery or other attacks. In V2G or VANET environment, since vehicles usually carry a lot of owner or user information, privacy-preserving is always a prerequisite.

3.2. Security and privacy-preserving technologies for physical objects in connection state

The security and privacy of physical objects in the connection state are usually achieved by authentication. Since IoT objects are always resource-constraint and usually have different roles in different environments, the authentication mechanisms are often required to be lightweight and flexible. Furthermore, privacy-preserving is also demanded during the authentication in many cases. There are mainly three security authentication schemes for securing the physical objects connecting to the IoT, which are batch authentication, dynamic authentication, and biometric authentication.

3.2.1. Batch authentication

Batch authentication schemes are often designed for bulk access mode, and their main purpose is to detect illegal or malicious physical objects trying to connect to the authenticator. Since different applications have different requirements for privacy protection, these batch authentication schemes are always designed for specific scenarios.

In an RFID system, the connection is often launched by the reader for reading data from tags. Since the connection is temporary, the communication resources and computation capabilities are very limited, most batch authentication schemes focus on efficiency and low overhead. And for security and privacy-preserving, the tag's sensitive data exchanged during the authentication is usually encrypted or blinded. Lei Yang et al. put forward a prompt and reliable batch authentication scheme for large scale RFID applications like anti-counterfeiting by verifying the validity of a batch of tags instead of identifying each tag [12], which can increase the efficiency significantly. Wei Gong et al. propose a fine-grained batch authentication scheme for large-scale RFID systems to address the scalability issue in batch authentications [13]. They use informative counting to lower the computation and communication costs, which can estimate the accurate numbers of counterfeiting tags and genuine tags. Liu et al. propose a Grouping-Proofs-Based Authentication (GUPA) protocol to address the security issue of simultaneously identifying multiple readers and tags in distributed RFID systems [14]. They adopt a distributed authentication mode with independent sub-grouping proofs to enhance hierarchical protection, use an asymmetric denial scheme to strengthen fault-tolerance capabilities for defending against the illegal/malicious reader or tag, and present a sequence-based odd-even alternation group subscript to define a lightweight function for secret updating.

In V2G and VANET environments, the characteristics of high speed, short communication range, and temporary connection require the aggregator (or roadside unit) and the vehicles to finish mutual authentication quickly [15]. At the same time, the privacy preservation is a prerequisite during the admission authentication. For these purposes, many batch authentication schemes are designed from different technical perspectives. Shunrong Jiang et al. put forward an efficient anonymous HMAC-based batch authentication scheme for VANETs to overcome the heavy overhead and privacy disclosure problems in PKI-based batch authentication [16,17]. They used Identity-Based Signature (IBS) and HMAC to realize batch authentication, and adopt pseudonyms to achieve conditional privacy-preserving. Huaqun Guo et al. put forward a batch authentication protocol [18,19] for V2G. The scheme in Ref. [19] is called Unique Batch Authentication Protocol for Vehicle-to-Grid (UBAPV2G). But Huei-Ru Tseng found that the batch authentication scheme UBAPV2G was not secure, and he pointed out that either the vehicle or aggregator can easily generate a collection of bogus signatures to make the batch verification succeed [20]. Liu H et al. thought that Battery Vehicles (BVs) had different security challenges when they work in different modes and proposed an Aggregated-proofs-based Privacy-preserving Authentication (AP3A) scheme to achieve batch authentication [21]. In addition, AP3A introduces the aggregated pseudo-status variation to collect multiple BVs' power status, since no individual data is revealed, and the privacy-preserving is achieved during the batch authentication.

3.2.2. Dynamic authentication

Dynamic authentication refers to the achievement of verification through different standards or certifications under different circumstances, which is the security basis for cross-domain access and ubiquitous connections. Furthermore, privacy-preserving is crucial in these scenarios, and the existing schemes for dynamic authentication are always required to provide privacy protection.

Hong Liu et al. designed two privacy protection authentication schemes for V2G networks in smart grids according to the battery status of electric vehicles [22] and their roles [23]. The former argues that there are three kinds of battery status, and different status faces different security and privacy problems. They use aggregate identifiers in the charging status to ensure that battery vehicles can be authenticated during the connection process without disclosing their real identities. At the same time, they employ the selective unblocking method to realize the anonymous data transmission when the vehicles are in the charging

status. In addition, they introduce aggregate-status during the status transition from discharging to charging, thereby hiding the vehicle's power from the aggregator. The latter classifies the battery vehicles into three roles of energy demander, energy storage, and energy supplier according to the battery status and proposes a role-dependent privacy--preserving scheme to achieve secure interactions between a vehicle and the smart grid. Refs. [22,23] Have some similarities in classification, but Ref. [23] focuses on designing the interlinked sub-protocols for battery vehicles to deal with the different privacy problems. Meanwhile, they also illustrated how to protect the vehicles' security and privacy in both the centralized and distributed discharging operations when a BV feeds energy back into the grid.

3.2.3. Biometric authentication

Biometric authentication is usually used in the scenario of physical objects accessing the unit IoT. Due to the uniqueness of some biometric characteristics, and they can be securely registered with the IoT in advance, the biometric authentication makes the physical object to access or connect to IoT conveniently. Since the invariance of biometric characteristics can ensure the consistency of the identities of the physical objects in physical space and IoT/cyberspace, the biometric authentication has distinct advantages in identifying the fake, malicious, and illegal nodes. For human beings, the common biometric proof may be the fingerprint, iris, face, etc. Pengfei Hu et al. put forward a face identification resolution framework based on the cloud [24] and fog [25] computing respectively for physical objects connecting to the IoT or being mapped from the physical space to cyberspace. At the same time, they also gave the corresponding security solution for the biometric data to preserve the object's privacy [25]. In addition, fingerprint and iris are often used for admission control. And for an IoT device, the biometric proofs are usually the fingerprint/digest or the pair of the challenge and response from its Physical Unclonable Function (PUF). The fingerprint/digest or PUF-based authentication schemes have similar ideas to those schemes based on the biometric data of human beings. Nevertheless, most PUF schemes focus on how to construct and use it to realize authentication, and how to deal with the noise generated by the PUF [26].

4. Security and privacy issues of physical objects in in-working

In the working stage, physical objects at different layers have different tasks and face different security and privacy problems. Furthermore, the same physical object may undertake different tasks in different spatiotemporal environment. Accordingly, their security and privacy requirements usually changes with the tasks and environments. So it is necessary and wise to study the physical objects' security and privacy problems according to their tasks instead of themselves. For clarity, we will first analyze the security and privacy requirements for physical objects in working according to their tasks and environments. And then, the corresponding security and privacy-preserving technologies or solutions will be surveyed by reviewing the related literature in detail.

4.1. Security and privacy requirements for physical objects in working

In general, the tasks of physical objects in working can be classified into data collection, data transmission, data processing, and data using. Accordingly, the security and privacy requirements will be analyzed from the four aspects.

4.1.1. Security and privacy requirements for data collection

There are two types of data collection. One is that a physical object (including the gateway and the normal nodes) or user collects the data from the object that undertakes the perceptual task, and the other is that physical objects act as the actuator or executor to receive the instructions from the control center, other physical objects or users.

The first type is the most common, where security and privacy threats are similar to those in wireless sensor networks, mainly including attacks on physical objects and their data. In addition, the attack on time synchronization cannot be ignored. Attacks on physical objects mainly include draining the battery of the sensing/sensing node working in the wrong mode, and being compromised as well. And the examples of attacks on the physical objects' data include eavesdropping, replaying, tampering, and even hijacking the perceived data during the data collection. Meanwhile, it is also a common attack to pretend to be a legitimate physical object to collect data and report false data to a legitimate data collector. All these threats or attacks may make the IoT system unavailable, reduce the accuracy, cause the leakage of perception data or the privacy of physical objects, lead to wrong decisions, and even put the related physical objects or users in danger. In order to ensure the safety of data collection, the following three requirements should be met.

Malicious physical object detection: The malicious physical object is the most harmful threat in data collection. Malicious physical object detection has two levels of meanings.

- The normal physical object should be able to identify the malicious/illegal physical object so as to resist the various attacks by itself and avoid the data/privacy leakage, which usually needs the help of fault/intrusion detection system and authentication mechanism.
- The normal physical object can differentiate between malicious requests and legitimate ones so as to avoid data/privacy leakage and wrong action. This ability is usually achieved by message or identity authentication mechanism.

Securing routing: Securing routing in data collection is responsible for sending the sensed data to the gateway and sending the control command to the specified executor, which is the basis of the successful data collection and should meet the following three requirements.

- The data can be routed to the destination correctly, which needs the support of the effective routing protocols.
- The integrity of the routed data should be kept, which is usually realized by cryptographic hash function or message authentication code.
- The data does come from the claimed physical object, which is essentially the requirement for the authenticity of the data source, and it can be guaranteed by signature or message authentication code.

Privacy preserving: In some cases of data collection, privacy-preserving is required by physical objects and/or users. For instance, the data in smart health is always required to be kept secret so as to protect the privacy and safe of patients. In general, the privacy requirement in data collection involves two aspects of data privacy-preserving and identity privacy-preserving.

- Data privacy-preserving requires the data to be kept secret from the unauthorized physical objects or users, which is usually achieved by encryption or access control mechanism.
- Identity privacy-preserving demands keeping the user or physical object's identity secret. Since the identity is always labeled by its related attribute data and can be deduced from these data, it is essentially required to keep the identity-related data secret. So anonymity, encrypting and blinding the related attribute data are the common way of preserving identity privacy.

For the second case of data collection, the instruction may come from malicious/illegal nodes and the wrong or malicious instructions may lead to incorrect behavior, data leakage, or even destruction or damage of the actuator/executor. Therefore, the legality, validity, authenticity and integrity of the instruction are of great importance. The physical objects (including the sensor, the actuator, or executor) that receive instructions

must be able to identify fake, illegal, or malicious instructions, so both the instruction and its senders have to be authenticated. At the same time, the sensitive or critical instructions are always required to be kept secret.

4.1.2. Security and privacy requirements for data transmission

Data transmission in physical objects' working status indicates transmitting the aggregated data from the gateway or other boundary nodes to the fog nodes, data center or control center, cloud, and so on. Similar to transmitting the private data over the public network, it is always required to ensure the data security, and the authenticity of the source and the destination. The authentication and end-to-end encryption mechanisms are the common solutions. Due to the diversity of the access networks, the variety and resource limitations of the gateway or boundary nodes, these common solutions cannot work well in data transmission, and the special security and privacy-preserving mechanisms are always required, which can be categorized into the following three kinds.

- Lightweight security transportation protocols, which is the basis of secure data transmission.
- Lightweight data security mechanism, including lightweight data integrity authentication and data encryption mechanism.
- Lightweight and flexible mutual authentication mechanism, which may be required to provide privacy-preserving simultaneously in some cases.

4.1.3. Security and privacy requirements for data processing

The security and privacy problems in data processing are mainly caused by intelligent computing and cloud computing technologies, such as data mining, outsource computing, and so on. Security problems mainly include data loss or leakage, and abuse as well. The privacy information that may be disclosed mainly includes the location, preferences, behaviors, identity, and others that may be derived from the sensed or aggregated data. So the data processing should meet the following two requirements.

- Secure cloud computing platform, which is not only the basis of secure data processing but also the foundation of secure data storage.
- The data processing algorithm with privacy-preserving, which is the basic method to avoid reasoning privacy.

4.1.4. Security and privacy requirements for data sharing

The security and privacy problems in data sharing are mainly caused by improper, few or no security restrictions on data sharing. At present, access control is a common and effective solution for secure data sharing, and there are many access control mechanisms that can meet data sharing requirements in different environments. In the IoT, the data to be shared may be on the cloud or in the physical object. For the former, most access control policies are designed either by the data owner or by both the owner and the cloud server. And the access to the data on the cloud is usually controlled by the cloud server instead of the data owner himself. Therefore, the security depends largely on the cloud server, and privacy may be breached unknowingly, which may further lead to serious problems. For the latter, data sharing can be controlled completely by the physical object itself, but resource limitations make the conventional access control mechanism unable to work normally. Whether sharing data in the cloud or physical objects, the data owner always wants to control it based on their own judgment. In order to share data securely with privacy-preserving, the access control schemes should have the following four characteristics [2].

- Automatical, autonomic access control means that the data owner can share its data as it wishes, or the access control policy can be made and performed by the data owner itself.
- Fine-grained, the fine-grained access control is the basis of ensuring the security of data sharing and privacy-preserving, which relies on the granularity of the data to be shared and the access control policy.
- Dynamic, the ever-changing IoT environment requires dynamic access control mechanism to achieve data sharing with minimum information leakage.
- Lightweight, the resource-limited physical object needs lightweight access control mechanism to share data, which is the guarantee of practicability.

It should be stated that dynamic and lightweight requirements for access control are also for the authentication in many data-sharing cases because access control mechanisms always depend on authentication.

4.2. Security and privacy-preserving technologies for physical objects in working

Corresponding to the security and privacy requirements analyses in Section 4.1, the security and privacy-preserving technologies for physical objects in working are summarized according to their tasks.

4.2.1. Security and privacy-preserving technologies for data collection

Security and privacy technologies for data collection can be categorized into four aspects of detection technology, key management, authentication and privacy-preserving.

Detection technology: The detection technology of data collection mainly includes fault detection and intrusion detection, which are used to distinguish the faulty physical object or malicious physical object from the normal ones. Currently, most existing solutions are designed for Wireless Sensor Networks (WSN), which are also suitable for the IoT. Different detection methods need different measures and techniques. The localized fault detection algorithm for identifying the faulty nodes in WSN [27], and the intrusion detection for homogeneous and heterogeneous WSNs [28] are the typical fault detection and intrusion detection, respectively. While Tie Qiu et al. come up with a safe time synchronization model to detect the malicious node so as to avoid the attack on timestamps or data replay [29]. With the rapid development of the IoT and the disappearance of boundaries, the typical detection technologies cannot work well in the perception layer [1]. In order to deal with this problem, artificial immunity and machine learning technologies are employed in fault or malicious physical objects identification. And the feature selection and modeling based on data mining are also introduced to locate the infected physical objects. These new Artificial Intelligent (AI) technologies are considered to be able to improve the conventional detection methods to a certain degree.

At the same time, intrusion tolerance technologies are used to reduce the harm caused by faulty or malicious physical objects, which can make the legitimate physical objects work well when there are temporarily inactive or permanently unavailable physical objects by making multiple physical objects collaborate together. An example is the data-driven robust algorithm for the IoT in smart cities, which is put forward by Tie Qiu et al. This algorithm uses the big data of smart cities to improve the robustness of topology against malicious attacks [9].

In addition, in order to resist attacks from malicious physical objects, the self-detection is becoming a necessary technology in the phase of physical object's design and booting [30]. For instance, some IoT devices have been designed to carry an error detection system, and some IoT devices are required to boot securely by authenticating the integrity of its software. It is very common in smartphones.

Key management: Key management is the basis of all the cryptography-based security and privacy-preserving schemes. Due to the nature of resource constraints, most of the existing key management technologies for IoT objects concentrate on lightweight, mainly including pre-distributed key schemes, public key-based key management schemes, and PUF-based key management scheme.

The pre-distributed key management scheme is very common and

usually used in the static case or initialization phase, such as the hexagon-based key pre-distribution scheme for large-scale static WSN in Ref. [31]. And the probabilistic key pre-distribution schemes are very popular, such as the random key chain pre-distribution [32] and the random pair-wise key scheme [33]. In addition, Zahid et al. put forward a distributed multi-party key management based on chaotic mapping and Chebyshev polynomial [34]. Nevertheless, the pre-distributed key management schemes always have many limitations, e.g., poor flexibility and low-security strength, which make them unfit for the physical objects in the distributed environment and ubiquitous IoT.

The public key-based key management scheme is relatively easy to implement in the distributed environment, but the overhead is a critical factor. Only the low-power public key encryption algorithms are promising candidates for IoT, such as elliptic curve cryptography [35,36]. In addition, there are other lightweight public key-based key management schemes designed for the distributed IoT application, such as PAuthKey [37], which uses implicit certificates and provides application-level end-to-end security.

The PUF-based key management uses the physical unclonable property of the circuit. Most of them are still based on the idea of Diffie-Hellman key exchange, but there is no need to exchange responses to generate keys. Furthermore, the PUF-based key does not need to be stored in the non-volatile memory, and will not be lost as the device is lost, because the key can be generated as needed. Although these advantages make the PUF-based key promising, it is hard to achieve in practical application. The current research focuses on how to generate the PUF key [38–44].

Authentication: In data collection, authentication is used to ensure the authenticity of the physical object and the integrity of the data. Due to the limitation of resources, most of the authentication schemes focus on lowering costs. For instance, Peris et al. [45] and Molnar et al. [46] propose two lightweight mutual authentication protocols for RFID tags and readers. The former claims that it can provide an adequate security level for certain applications at the cost of slightly more than 300 gates, and the latter uses shared secret and pseudo-random functions to ensure the integrity and authenticity of messages exchanged between tags and readers. In order to meet the high security and reliability requirements for data in smart health, Wei Liu et al. [47] put forward a yoking-proof-based authentication protocol for cloud-assisted wearable devices. They use a physical unclonable function and lightweight cryptographic operators to realize mutual authentication between a smartphone and two wearable devices. Hong Liu et al. [48] introduced the hash-based selective disclosure mechanism and Chebyshev chaotic map to achieve mutual authentication between a wearable device and a smartphone.

At the same time, the multicast is the main communication mode in IoT data collection, and lightweight multicast authentication is indispensable. Since the receivers of multicast data usually do not trust each other, the multicast authentication mechanisms are usually based on asymmetric methods. The common multicast authentication schemes include public key-based multicast authentication schemes [49,50]; symmetric key-based multicast authentication schemes [51,52]; and one-time signature-based authentication schemes [53,54]. The first and the last are inherently asymmetric. And the second is essential to construct an asymmetric property on the symmetric key and one-way hash function. Due to the limited resources and the distributed environment, neither public key nor one-time signature-based schemes can work well for IoT data collection. The symmetric key-based multicast authentication scheme is the preferred one. For different scenarios, there are different symmetric key-based multicast authentication schemes. For instance, Xuanxia Yao et al. put a lightweight multicast authentication mechanism based on the revised Nyberg's fast one-way accumulator for small scale multicast applications [55], which enables the data sender to specify the data receivers, and the data receivers are able to verify the authenticity of a data source at low cost.

Privacy preserving: Privacy-preserving technologies used in data collection mainly include encryption, anonymity, obfuscation, data aggregation, and onion routing as well.

Encryption is a usual way to maintain data privacy. Since the data is directly encrypted, privacy is naturally preserved. There are two situations for anonymity. One is that the data is reported by an anonym, and the anonymous data reporting protocol proposed by Yao et al. [56] is a typical example. The other method is to anonymize the data before submitting it to the collectors, which is essentially similar to obfuscation and always combined with data aggregation. There are many works on anonymous data aggregation, including anonymous grouping message [57], Grouping-proofs-based authentication [58], aggregated proofs-based authentication [21], and anonymous message submission [59]. Their common purpose is to prevent the data collector from tracking the submitter.

Onion routing is designed to prevent privacy leakage caused by the traffic analysis. Since the backward and forward routing is anonymous, it cannot be tracked, and the privacy of the source and the destination is preserved. At the same time, all kinds of attacks based on the routing can be avoided by the obfuscated or anonymized routing data.

4.2.2. Security and privacy-preserving technologies for data transmission

Security and privacy-preserving technologies for data transmission are mainly a variety of authentication protocols and secure transport protocols with the characteristic of lightweight. The former is used to verify the legality of the data sender and receiver [47,48], which have been analyzed at length in data collection. And the latter is designed for sending data to the remote data center or cloud, which usually covers encryption, authentication, and integrity check. In practice, these technologies are not always required. For instance, privacy-preserving is optional in environmental monitoring but is a prerequisite in smart health.

The long-distance data transmission is often based on IP communication, IPv6 over low-power personal area networks (6LoWPAN) is a good choice, which can carry out IPSec on IPv6 nodes (such as the edge physical object or the gateway) to make them communicate with the data or control center safely without any modification on them. And many end-to-end secure transport protocols are designed on it. For instance, Raza et al. [60] extend the low-power personal area networks (LoWPAN) to support the IPSec's Authentication Header (AH) and Encapsulation Security Payload (ESP) simultaneously for securing the data transmission from the aspects of confidentiality, authenticity and integrity. Granjal et al. [61] employ the 6LoWPAN security headers to realize end-to-end security between the edge physical object/gateway and the data/-control center.

In addition, the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocol are also common ways to secure data transmission. And there are many schemes based on DTLS. For instance, Dos Santos et al. [62] use DTLS to construct an architecture for secure communication between the resource-constraint IoT entities. And Kothmayr et al. [63] design a two-way authentication scheme based on DTLS. Since these schemes do not only focus on the confidentiality, authenticity and integrity of the communication but also take the limited resources into account, they can perform well in securing IoT data transmission.

4.2.3. Security and privacy-preserving technologies for data processing

Security and privacy-preserving technologies for data processing mainly include homomorphic computing, secure multiparty computing, and data mining with privacy-preserving as well. These technologies are always cross-used to solve the security and privacy problems in data processing.

The homomorphic computing and secure multiparty computing technologies are very helpful in addressing the security and privacy problems in data processing, especially in the calculation. Qian Ping et al. surveyed the privacy-preserving technologies in the IoT [64] and pointed out that the homomorphic encryption is very effective for privacy

preservation in computational data processing. There are many studies on homomorphic encryption and secure multi-party computing, but most of them are not practical in data analysis, classification, feature extraction, and the alike data processing. On the contrary, the data mining algorithm with privacy-preserving is much effective to deal with the non-computational data processing. The privacy-preserving decision trees over vertically partitioned data is a typical one [65], which can achieve data classification and privacy-preserving simultaneously. And Yang et al. try to use the bayesian network to realize privacy-preserving computation for vertically partitioned data [66].

4.2.4. Security and privacy-preserving technologies for data sharing

Security and privacy-preserving technologies for data-sharing are usually a variety of access control mechanisms. Since data sharing is always closely related to the application, most of the existing schemes are designed for specific scenarios with the purpose of meeting the requirements for autonomy, fine-granularity, dynamics, and lightweight.

For various data-sharing requests, a hierarchical access control mechanism is always required. Liu H et al. put forward an aggregated-proof-based hierarchical authentication scheme for the IoT [67], which uses the directed path descriptors, homomorphism functions, and Chebyshev chaotic maps jointly to achieve the mutual authentication. Based on it, the hierarchical access control is achieved by assigning different access authorities to different data users. Since the proofs are aggregated, the privacy is preserved simultaneously.

For data sharing in the cloud, since different physical objects may have a collaborative relationship, both achieving common security and privacy-preserving and meeting the individual's security and privacy-preserving requirements are of very importance. Most of the existing solutions focus on keeping the physical object's private data from unauthorized access by authentication, but the privacy of the physical object that requests data sharing is always ignored. To preserve the privacy of the data requestor, H Liu and H Ning et al. propose a shared authority-based privacy-preserving authentication protocol for data sharing in the cloud [68]. They use the anonymous access request matching mechanism to share access authority; employ the attribute-based access control to realize fine-grained and automatic access control; apply proxy re-encryption to keep the security for the dynamic data sharing. Xuanxia Yao et al. present an anonymous credential-based access control scheme to share the data in the cloud [69], which can achieve a flexible and lightweight cipher text sharing. And at the same time, the physical object that makes the data sharing request is kept anonymous. In addition, Hong Liu et al. put forward the cooperative privacy preservation in authentication and access control for the wearable devices in hybrid (edge and cloud) computing environment [70]. It can meet the secure data sharing and privacy-preserving requirements for physical objects in the dynamic environment.

For data sharing in the physical object, Xuanxia Yao et al. design a lightweight attribute-based encryption scheme based on Elliptic Curve Cryptography (ECC) [2], which can avoid using bilinear pair mapping to realize lightweight, and construct the access control policy according to the access tree and perform an access control of attribute-based encryption to achieve a flexible, dynamic and fine-grained access control.

5. Security and privacy issues of physical objects in post-working

In the stage of post-working, physical objects are generally idled or discarded. In most cases, their security and privacy problems are often ignored by their owners, which make them vulnerable to being attack targets (such as being captured, compromised, or reused by attackers) and face serious security threats and privacy leakage challenges. For clarity, the security and privacy-preserving requirements of the physical objects in post-working are also firstly analyzed in detail. And then, the security and privacy-preserving technologies for physical objects in post-working will be surveyed by reviewing the related literature.

5.1. Security and privacy requirements of physical objects in post-working

In general, there are three kinds of situations for a physical object in post-working. 1) It will be captured by an attacker when it has retired or is working. 2) It has been damaged or malfunctions. 3) It is normally retired from the IoT. The first two situations are abnormal or passive withdrawal from the IoT. And physical objects in the first situation are completely out of the control of its owner or user, and its data may be stolen by attackers. Of course, they may be reconnected to the IoT by attackers. Meanwhile, physical objects in the second situation may be repaired and sent back to the IoT by legal or illegal users. Similar to the first two situations, physical objects in the third situation may also enter the IoT under specific circumstances. In summary, the physical objects re-accessing the IoT can be classified into two categories: normal nodes and replay nodes.

For all three situations, the possible attacks on physical objects in post-working can be roughly classified into three kinds: physical attack, data theft, and replay attacks. In essence, the last two attacks are usually the targets of the first one. The physical attack is often launched directly by capturing the target. And stealing/obtaining data from the physical object in post working is usually realized by physically or logically decomposing the captured objects. The replying attack has two meanings: one is to try to use the captured physical object in post working to access the IoT for getting the unauthorized data and services, or for attacking the IoT itself. The other meaning is to reuse its data to create a fake physical object to access the IoT.

Accordingly, the security and privacy requirements can be summarized into physical security, data security and replaying detection.

- Physical security: Physical security refers to keep the physical objects in a safe environment or far from being captured by illegal/malicious users. Since the retired physical objects are always ignored, they are vulnerable to being captured and utilized by attackers, and further threaten the security and privacy of the working physical objects and the IoT. The physical security is the foundation of the physical objects' security.
- Data security: In most cases, the purpose of capturing a physical object is to obtain its data or tamper with its data to obtain unauthorized data and services. The captured physical objects may be a normal cyber entity, a damaged physical object, or a retired one. And the latter two are more common because they are usually ignored and easily captured. No matter what kind the captured physical object is, its data is always closely related to the security of the application and the privacy of the physical object itself or its users. The disclosure of these data will threaten not only the security and privacy of the object and its user, but also the security of the IoT and the corresponding application, and even lead many related physical objects to leak their sensitive data. It can be said that data security is the basic and crucial requirement to ensure the security and privacy of the physical objects in post-working, which requires their data to be kept secret from, or not to be leaked to, any unauthorized objects.
- Replaying identification or detection: The corrupted or the fake physical object is always used by the illegal user to reconnect to the IoT. We call it physical object replaying. And the retired or the repaired physical objects may be reused to work by the authorized users, which is treated as reworking instead of replaying. Identifying the replayed physical object from the normal ones (reworking and normally working objects) is crucial to the security of the IoT.

5.2. Security and privacy-preserving technologies for physical objects in post-working

The security and privacy technologies for physical objects in post-working are designed to meet the security and privacy requirements analyzed in Section 5.1. For physical security, it is usually guaranteed by physical measures and management means. Both of them are to

strengthen physical protection to ensure the retried or damaged physical objects in a safe environment or prevent them from being captured by attackers. Since it is beyond the security and privacy-preserving technical specification, it is not discussed here. For replaying detection or identification, it is essentially the security issues of the physical objects in pre-working or during connecting to the IoT, which is usually achieved by authentication. Since it has been discussed in Section 3, we just focus on the technologies to ensure the captured, damaged and retired physical objects' data security. There are roughly two directions, which are hardware-oriented technologies and software-oriented technologies.

5.2.1. Hardware-oriented technologies for data security

Hardware-oriented security and privacy-preserving technologies are generally used to destroy the objects physically when they run abnormally. The purpose of the physical destruction is to make the captured physical objects unable to re-access the IoT and their data unable to be read out. There are roughly two directions, which are transient electronics-based methods and circuit-based methods.

Transient electronics is a promising technology for self-deciding the death of the chip, which explores the characteristics of water solubility or chemical corrosion of transient materials, so that the chip will physically disappear or function to self-destruct in a controlled and triggered manner [71]. The water-soluble transient materials are mainly used in fields where the security requirement is very high, and the unused or abandoned physical objects are required to vanish, such as military and medicine. The chemically corrosive agent is usually used to disrupt the function of the physical object, and the microfluidic system or Micro-Fluidic Self-destruct Device (MFSD) is designed to destroy the structure and the data of the microchip in an abnormal environment [72]. Xinwei Gu et al. put forward a self-absorption and self-destruct system based on micro-fluidic for the memory chip according to the characteristics of the abnormal environment and conducted a simulation research on the new MFSD for microchips [73]. In their simulation, the system is able to generate a chemical preparation and spray it on the chip to destruct the structure of the chip and erase the data in the memory permanently when it senses that it is disassembled. Thereby, the structure and the data of the device will not be disclosed even it is disassembled. Of course, the device cannot be used by an attacker to re-connect the IoT.

The circuit-based methods are usually achieved by the open circuit or short circuit and can be controlled by external operation or command. Jin-Woo Han et al. presented a self-destructible fin flip-flop actuated channel transistor, which applies a trigger voltage to a trigger gate mechanically for generating electrostatic bending stress to shatter the source/drain extension region of the fin [74]. Since an open circuit at the individual transistor level is formed, the designed function of the chip is destroyed. The Micro-electromechanical Systems (MEMS) initiator is a micro detonating device with low detonating power and small volume, which is widely used in many fields [75,76]. It is also a solution to realize the Application Specific Integrated Circuit (ASIC) self-destruction. The circuits of the ASIC will be destroyed immediately when the MEMS metal bridge is excited by a pulse current. Zhao Yue et al. presented a novel ASIC self-destruction technology at the chip level by integrating the MEMS metal bridge initiator and the ASIC [77]. It can destruct the ASIC when receiving the command for destroying the device. Consequently, the related device or physical object cannot be utilized by malicious or illegal users.

In addition to mechanical trigger and command, both of the two self-destruction technologies may be driven by the energy of the node in the wireless sensor network so as to destroy it timely [78]. Meanwhile, letting the malicious nodes self-destruct can also protect the physical objects [79].

5.2.2. Software-oriented technologies for data security

Software-oriented security and privacy technologies for the physical objects in post-working mainly include encryption schemes and access control mechanisms. Both of them are designed to ensure that the (sensitive) data can only be accessed by the legally authorized users in a specific time interval and environment, but thoroughly unreadable/unrecoverable for all unauthorized users.

Encryption schemes: As the basic means of data security and privacy-preserving, encryption is also a common method for protecting the physical objects in post-working. The basic idea is to store the data in cypher-text and destroy the decryption key after a certain time. Without the decryption key, unauthorized users cannot recover the data in the captured physical objects. Consequently, the data security and privacy can be preserved. At the same time, an attacker is unable to exploit the captured physical object to reconnect to the IoT because their data are no longer available without the decryption key. And the replay attacks can also be avoided.

In practice, the encryption schemes are always closely related to the applications. Radia Perlman tried to make the data of physical objects in post-working unrecoverable after a specific time by putting all key operations (including key creating, key using and key destroying) in one place [80]. Essentially, it is a centralized key management approach, which is not appropriate for the distributed IoT environment. In cloud-based IoT, most of physical objects' data are often stored in the cloud. And the attribute-based encryption mechanism [81,82] and Distributed Hash Table (DHT) [83,84] are two common approaches for protecting the physical objects in post-working. In addition, the methods of combining different technologies are also very common. Lingfang Zeng et al. put forward a self-destructing data system by integrating the cryptographic techniques with active storage techniques [85]. Jinbo Xiong et al. combined the IDentity-based Timed-Release Encryption (IDTRE) algorithm with the distributed hash table to realize full lifecycle privacy-preserving [84].

Access control mechanisms: For physical objects in post-working, access control is always the prerequisite for their security and privacy-preserving. And authentication is generally the basis of access control. Due to the resource constraints, both the authentication and access control are required to be lightweight. In order to limit the access or reuse of the data of the physical objects in post-working, biometric information and device fingerprints are often used to achieve authentication and access control. For instance, PUF-based authentication protocols are often used to identify the unauthorized access requesters, which can ensure the authenticity of the accessor and achieve access control on physical objects in all stages. The existing research on PUF-based authentication mainly focuses on two directions: One is error correction methods [26], and the other is how to construct a PUF or how to generate the response to a challenge [86]. In practice, PUF may be combined with the user's biometric or intrinsic attributes to achieve access control [87], and used with cryptographic technologies to complete device authentication [88] as well.

6. Challenges and future directions

The rapid development of microelectronics technology has made the size of IoT objects smaller and smaller, the form/structure more and more diverse, and the functions more and more abundant. At the same time, cloud computing and edge computing technologies provide IoT objects with efficient computing, storage, and latency solutions. As a result, ubiquitous computing enabled by IoT has been widely used in various fields. In the environment of everything interconnecting, physical objects have to face many new security and privacy challenges. Meanwhile, the booming microelectronics technology, biometric information technology, and cryptographic technology also give promising directions for security and privacy-preserving technologies. In order to figure out the security and privacy challenges faced by physical objects and explore future directions, the related works are summarized and compared in Table 1.

Table 1
Related research: Summary and comparison.

Refs	Physical objects' status	Security Goals	Methods or Technologies	Privacy preserving	Lightweight	Scenarios
[1,6–30, 64]	All	Survey	Survey			U2IoT/IoT
[10–14]	Batch connection	anti-counterfeiting security access fault tolerance	Batch authentication	✓	✓	RFID system
[15–17]	Batch connection	Security access	Batch verification	✓	✓	VANET
[18–23]	Batch connection	Security access	Batch authentication	✓		V2G
[24–26]	Single connection	Security access	Biometric/PUF authentication		✓	Cloud, Fog based IoT
[9,27,28]	Data collection	Fault/Intrusion detection	Comparison/Data-driven			WSN Smart city
[31–33]	In working	Key Gen	Pre-key distribution		✓	WSN, IoT
[35–37]	In working	Key Gen	Public key			WSN, IoT
[38–44]	In working	Key Gen	PUF key		✓	IoT
[45,46]	In working	Objects Authenticity	Mutual authentication	✓	✓	RFID system
[47,48]	In working	Objects Authenticity	Mutual authentication	✓	✓	Cloud/fog based BAN
[49,50,53, 54]	Data collection	Authenticity of data sources	Public key/one-time signature-based Multicast authentication			General
[51,52,55]	Data collection	Authenticity of data sources	Symmetric key based Multicast authentication		✓	WSN, IoT
[56,57,59]	Data collection	Legality of data sources	Anonymous authentication	✓		IoT
[21,58]	Data collection	Legality of objects	Proof-aggregated authentication	✓	✓	IoT
[60–63]	Data transmission	End-to-end data security	6LOWPAN DTLS		✓	WSN Ad Hoc
[65,66]	Data processing	Prevent inference privacy	Data partitioned vertically	✓		Data classification
[2,67–70]	Data sharing	Secure data sharing	Anonymous access control	✓	✓	IoT
[71–79]	Post-working	Data security, IoT security	Device self-destruct	✓		Military, medical applications
[80–85]	Post-working	Data security, IoT security	Data destroy	✓		Military, medical applications
[86–88]	Post-working	Data security, IoT security	Access control	✓		PUF devices
[89,90]	All	Objects management	Block chain			Ubiquitous IoT

6.1. Challenges

According to Table 1 and the analyses in Section 2, 3, 4 and 5, security and privacy challenges that physical objects may face in ubiquitous IoT can be categorized into seven aspects.

- Both the conventional pre-distributed key management method and the public key-based key management scheme cannot work well in the IoT-based pervasive computing environment. Since any two strange physical objects may need to communicate with each other at any time, all static key management schemes and those based on the trusted third party schemes are unable to meet their requirements for the random or dynamic key negotiation, which further limits the data exchange and brings serious security and privacy problems.
- The edge computing-based IoT faces many new security and privacy vulnerabilities. As the bridge between the cloud and the perception network, the edge node is close to not only the data source but also the local data centers, which make it the attack target, and its related sensitive information be vulnerable to leakage.
- The completely distributed and highly dynamic environment of the IoT-enabled ubiquitous computing needs to balance the relations among the service, security and privacy as well. Better service and stronger security always need detailed personal data, but higher privacy demands minimum data disclosure, which makes the existing static security and privacy technologies cannot well meet the dynamic security and privacy-preserving requirements of the physical objects.
- The IoT-based ubiquitous computing often needs data sharing and data use across security domain or unit IoT, which makes the sharing and use of sensitive data face very complex security and privacy issues. For instance, How can a data owner effectively outsource its data with confidentiality?
- A physical object often needs to communicate with an unfamiliar object in another different security domain. The establishment of a basic trust relationship for the two physical objects that do not know each other is the foundation of their security and privacy.
- How to prevent unauthorized users from accessing physical objects is the basis for ensuring the security and privacy of the objects and their owner. Although using the biometric information to bind the physical objects with its owner is a popular solution, there are still many new security and privacy problems to be solved.
- With the development of blockchain, it seems to be a trend to use blockchain to manage physical objects [89]. Nevertheless, the public ledger makes the users have to face the new security and privacy breach challenges.

6.2. Future directions

There are many open issues published for advice or solutions to deal with confronting and emerging security and privacy challenges. In summary, the following seven directions are worthy of further study.

- With the development of a microelectronic technique, it is a promising option to study the security of IoT devices from the design phase, which can protect the physical objects from the physical or hardware perspective.
- The dynamic, lightweight, and flexible key management scheme is the foundation to meet the security and privacy requirements of the physical objects in the distributed, large-scale IoT or ubiquitous computing environment.
- Using machine learning and data mining technology to obtain or predict the privacy and security requirements of physical objects in context is a promising solution, which further makes it possible to provide dynamic security and privacy-preserving as required.
- As a distributed and tamper-resistant ledger, blockchain is a promising technology to provide security solutions for IoT [90], including managing and securing the IoT data and devices. It is urgent to study how to preserve the physical objects and their users' privacy while securing their security on the blockchain.
- Letting the physical objects design, manage the access control policy by themselves and directly control who can access their data is an ideal solution to secure data and preserve privacy, which requires an autonomous access control mechanism.
- An efficient, fully homomorphic encryption scheme can meet the requirements of sensitive data sharing and use. It is the basis of

ensuring the security and privacy of the physical objects in cloud-based IoT and edge computing-based IoT.

- A lightweight, secure multiparty computation scheme is an effective way to establish a basic trust relationship for two strange physical objects, which is a common problem that needs to be solved urgently in ubiquitous IoT.

7. Conclusion

In order to solve the complicated, dynamic and numerous security and privacy problems of physical objects in the IoT, the life cycle of physical objects is divided into three stages: pre-working, in-working, and post-working. According to the physical object's working status, an IoT security architecture is put forward. From the perspective of analyzing the security and privacy requirements of physical objects in different working status/stage, the corresponding security and privacy-preserving technologies are surveyed and sorted out. On this basis, the challenges and future research directions for the security and privacy issues of physical objects are also analyzed and summarized. Since the security and privacy-preserving technologies for physical objects in IoT can also be applied to the entities in other networks, the survey is also helpful to protect the physical objects in the whole cyberspace.

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grant 61872038, 61811530335, and in part by the UK Royal Society-Newton Mobility Grant (No.IEC\NSFC\170067).

References

[1] H. Ning, H. Liu, L.T. Yang, Cyberentity security in the internet of things, Computer 46 (4) (2013) 46–53.
[2] X. Yao, Z. Chen, Y. Tian, A lightweight attribute-based encryption scheme for the internet of things, Future Generation Computer Systems 49 (2015) 104–112.
[3] P. Hu, H. Ning, L. Chen, M. Daneshmand, An open internet of things system architecture based on software-defined device, IEEE Internet of Things Journal 6 (2) (2019) 2583–2592, https://doi.org/10.1109/JIOT.2018.2872028.
[4] Z. Mahmood, H. Ning, A. Ullah, X. Yao, Secure authentication and prescription safety protocol for telecare health services using ubiquitous iot, Appl. Sci. 7 (10) (2017) 1069, https://doi.org/10.3390/app7101069.
[5] I. Psychoula, D. Singh, L. Chen, F. Chen, A. Holzinger, H. Ning, Users' privacy concerns in iot based applications, in: 2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2018, pp. 1887–1894, https://doi.org/10.1109/SmartWorld.2018.00317.
[6] B.V.S. Krishna, T. Gnanasekaran, A systematic study of security issues in internet-of-things (iot), in: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 107–111, https://doi.org/10.1109/I-SMAC.2017.8058318.
[7] Y. Chahid, M. Benabdellah, A. Azizi, Internet of things security, in: 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), 2017, pp. 1–6, https://doi.org/10.1109/WITS.2017.7934655.
[8] H. Ning, H. Liu, Cyber-physical-social based security architecture for future internet of things, Adv. Internet Things 2 (2012) 1, 01.
[9] T. Qiu, J. Liu, W. Si, M. Han, H. Ning, M. Atiquzzaman, A data-driven robustness algorithm for the internet of things in smart cities, IEEE Commun. Mag. 55 (12) (2017) 18–23, https://doi.org/10.1109/MCOM.2017.1700247.
[10] X. Zhang, B. King, An anti-counterfeiting rfid privacy protection protocol, J. Comput. Sci. Technol. 22 (3) (2007) 438–448.
[11] S. Choi, C. Poon, An rfid-based anti-counterfeiting system, IAENG Int. J. Comput. Sci. 35 (1) (2018).
[12] L. Yang, J. Han, Y. Qi, Y. Liu, Identification-free batch authentication for rfid tags, in: The 18th IEEE International Conference on Network Protocols, IEEE, 2010, pp. 154–163.
[13] W. Gong, K. Liu, X. Miao, Q. Ma, Z. Yang, Y. Liu, Informative counting: fine-grained batch authentication for large-scale rfid systems, in: Proceedings of the Fourteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing, ACM, 2013, pp. 21–30.
[14] H. Liu, H. Ning, Y. Zhang, D. He, Q. Xiong, L.T. Yang, Grouping-proofs-based authentication protocol for distributed rfid systems, IEEE Trans. Parallel Distr. Syst. 24 (7) (2012) 1321–1330.
[15] M. Bayat, M. Barmshoory, M. Rahimi, M.R. Aref, A secure authentication scheme for vanets with batch verification, Wireless Network 21 (5) (2015) 1733–1743.
[16] S. Jiang, X. Zhu, L. Wang, An efficient anonymous batch authentication scheme based on hmac for vanets, IEEE Trans. Intell. Transport. Syst. 17 (8) (2016) 2193–2204.
[17] Z.X. Jiang, Shunrong, L. Wang, A conditional privacy scheme based on anonymized batch authentication in vehicular ad hoc networks, in: 2013 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, 2013, pp. 2375–2380.
[18] H. Guo, Y. Wu, H. Chen, M. Ma, A batch authentication protocol for v2g communications, in: 2011 4th IFIP International Conference on New Technologies, Mobility and Security, IEEE, 2011, pp. 1–5.
[19] H. Guo, Y. Wu, F. Bao, H. Chen, M. Ma, Ubapv2g: a unique batch authentication protocol for vehicle-to-grid communications, IEEE Transactions on Smart Grid 2 (4) (2011) 707–714.
[20] H.-R. Tseng, On the security of a unique batch authentication protocol for vehicle-to-grid communications, in: 2012 12th International Conference on ITS Telecommunications, IEEE, 2012, pp. 280–283.
[21] H. Liu, H. Ning, Y. Zhang, L.T. Yang, Aggregated-proofs based privacy-preserving authentication for v2g networks in the smart grid, IEEE Transactions on Smart Grid 3 (4) (2012) 1722–1733.
[22] H. Liu, H. Ning, Y. Zhang, M. Guizani, Battery status-aware authentication scheme for v2g networks in smart grid, IEEE Transactions on Smart Grid 4 (1) (2013) 99–110.
[23] H. Liu, H. Ning, Y. Zhang, Q. Xiong, L.T. Yang, Role-dependent privacy preservation for secure v2g networks in the smart grid, IEEE Trans. Inf. Forensics Secur. 9 (2) (2013) 208–220.
[24] P. Hu, H. Ning, T. Qiu, Y. Xu, X. Luo, A.K. Sangaiah, A unified face identification and resolution scheme using cloud computing in internet of things, Future Generation Computer Systems 81 (2018) 582–592.
[25] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, X. Yao, Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things, IEEE Internet of Things Journal 4 (5) (2017) 1143–1155.
[26] M. Zhao, X. Yao, H. Liu, H. Ning, Physical unclonable function based authentication protocol for unit iot and ubiquitous iot, in: 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), IEEE, 2016, pp. 179–184.
[27] J. Chen, S. Kher, A. Somani, Distributed fault detection of wireless sensor networks, in: Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, ACM, 2006, pp. 65–72.
[28] Y. Wang, X. Wang, B. Xie, D. Wang, D.P. Agrawal, Intrusion detection in homogeneous and heterogeneous wireless sensor networks, IEEE Trans. Mobile Comput. 7 (6) (2008) 698–711.
[29] T. Qiu, X. Liu, M. Han, H. Ning, D.O. Wu, A secure time synchronization protocol against fake timestamps for large-scale internet of things, IEEE Internet of Things Journal 4 (6) (2017) 1879–1889, https://doi.org/10.1109/JIOT.2017.2714904.
[30] Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, A survey on security and privacy issues in internet-of-things, IEEE Internet of Things Journal 4 (5) (2017) 1250–1258.
[31] X. Yao, X. Zheng, T. Wu, A hexagon-based key pre-distribution scheme for large scale static wireless sensor networks, JCM 3 (6) (2008) 19–26.
[32] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, ACM, 2002, pp. 41–47.
[33] H. Chan, A. Perrig, D. Song, Random Key Predistribution Schemes for Sensor Networks. doi:10.1184/R1/6469211.v1.
[34] Z. Mahmood, A. Ullah, H. Ning, Distributed multiparty key management for efficient authentication in the internet of things, IEEE Access 6 (2018) 29460–29473.
[35] G. Gaubatz, J.-P. Kaps, E. Ozturk, B. Sunar, State of the art in ultra-low power public key cryptography for wireless sensor networks, in: Third IEEE International Conference on Pervasive Computing and Communications Workshops, IEEE, 2005, pp. 146–150.
[36] E. Öztürk, B. Sunar, E. Savaş, Low-power elliptic curve cryptography using scaled modular arithmetic, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2004, pp. 92–106.
[37] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, M. Ylianttila, Pauthkey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications, Int. J. Distributed Sens. Netw. 10 (7) (2014) 357430, https://doi.org/10.1155/2014/357430.
[38] Y. Dodis, L. Reyzin, A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, in: C. Cachin, J.L. Camenisch (Eds.), Advances in Cryptology - EUROCRYPT 2004, Springer Berlin Heidelberg, Berlin, Heidelberg, 2004, pp. 523–540.
[39] R. Maes, A. Van Herrewege, I. Verbauwhede, Pufky: a fully functional puf-based cryptographic key generator, in: E. Prouff, P. Schaumont (Eds.), Cryptographic Hardware and Embedded Systems – CHES 2012, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 302–319.
[40] Z. Paral, S. Devadas, Reliable and efficient puf-based key generation using pattern matching, in: 2011 IEEE International Symposium on Hardware-Oriented Security and Trust, 2011, pp. 128–133, https://doi.org/10.1109/HST.2011.5955010.
[41] Daihyun Lim, J.W. Lee, B. Gassend, G.E. Suh, M. van Dijk, S. Devadas, Extracting secret keys from integrated circuits, IEEE Trans. Very Large Scale Integr. Syst. 13 (10) (2005) 1200–1205, https://doi.org/10.1109/TVLSI.2005.859470.
[42] G.E. Suh, S. Devadas, Physical unclonable functions for device authentication and secret key generation, in: 2007 44th ACM/IEEE Design Automation Conference, 2007, pp. 9–14.
[43] C. Bösch, J. Guajardo, A.-R. Sadeghi, J. Shokrollahi, P. Tuyls, Efficient helper data key extractor on fpgas, in: E. Oswald, P. Rohatgi (Eds.), Cryptographic Hardware

and Embedded Systems – CHES 2008, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 181–197.
[44] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, SIAM J. Comput. 38 (1) (2008) 97–139, https://doi.org/10.1137/060651380, doi:10.1137/060651380.
[45] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, M 2 ap: a minimalist mutual-authentication protocol for low-cost rfid tags, in: International Conference on Ubiquitous Intelligence and Computing, Springer, 2006, pp. 912–923.
[46] D. Molnar, D. Wagner, Privacy and security in library rfid: issues, practices, and architectures, in: Proceedings of the 11th ACM Conference on Computer and Communications Security, ACM, 2004, pp. 210–219.
[47] W. Liu, H. Liu, Y. Wan, H. Kong, H. Ning, The yoking-proof-based authentication protocol for cloud-assisted wearable devices, Personal Ubiquitous Comput. 20 (3) (2016) 469–479, https://doi.org/10.1007/s00779-016-0926-8.
[48] H. Liu, H. Ning, Y. Yue, Y. Wan, L.T. Yang, Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices, Future Generation Computer Systems 78 (2018) 976–986, https://doi.org/10.1016/j.future.2017.04.014.
[49] K. Ren, S. Yu, W. Lou, Y. Zhang, Multi-user broadcast authentication in wireless sensor networks, IEEE Trans. Veh. Technol. 58 (8) (2009) 4554–4564.
[50] X. Cao, W. Kou, L. Dang, B. Zhao, Imbas: identity-based multi-user broadcast authentication in wireless sensor networks, Comput. Commun. 31 (4) (2008) 659–667.
[51] K. Ren, W. Lou, K. Zeng, P.J. Moran, On broadcast authentication in wireless sensor networks, IEEE Trans. Wireless Commun. 6 (11) (2007) 4136–4144.
[52] D. Liu, P. Ning, Multilevel μtesla: broadcast authentication for distributed sensor networks, ACM Trans. Embed. Comput. Syst. 3 (4) (2004) 800–836.
[53] S.-M. Chang, S. Shieh, W.W. Lin, C.-M. Hsieh, An efficient broadcast authentication scheme in wireless sensor networks, in: Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, ACM, 2006, pp. 311–320.
[54] X. Fan, G. Gong, Accelerating signature-based broadcast authentication for wireless sensor networks, Ad Hoc Netw. 10 (4) (2012) 723–736.
[55] X. Yao, X. Han, X. Du, X. Zhou, A lightweight multicast authentication mechanism for small scale iot applications, IEEE Sensor. J. 13 (10) (2013) 3693–3701.
[56] Y. Yao, L.T. Yang, N.N. Xiong, Anonymity-based privacy-preserving data reporting for participatory sensing, IEEE Internet of Things Journal 2 (5) (2017) 381–390.
[57] H. Corrigan-Gibbs, B. Ford, Dissent:accountable anonymous group messaging, in: Acm Conference on Computer & Communications Security, 2010.
[58] L. Hong, H. Ning, Z. Yan, D. He, Q. Xiong, L.T. Yang, Grouping-proofs-based authentication protocol for distributed rfid systems, IEEE Trans. Parallel Distr. Syst. 24 (7) (2013) 1321–1330.
[59] X. Zhao, L. Li, G. Xue, G. Silva, Efficient anonymous message submission, in: 2012 Proceedings IEEE INFOCOM, IEEE, 2012, pp. 2228–2236.
[60] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, U. Roedig, Securing communication in 6lowpan with compressed ipsec, in: International Conference on Distributed Computing in Sensor Systems & Workshops, 2011.
[61] J. Granjal, E. Monteiro, J.S. Silva, A secure interconnection model for ipv6 enabled wireless sensor networks, in: 2010 IFIP Wireless Days, IEEE, 2010, pp. 1–6.
[62] G.L. dos Santos, V.T. Guimarães, G. da Cunha Rodrigues, L.Z. Granville, L.M.R. Tarouco, A dtls-based security architecture for the internet of things, in: 2015 IEEE Symposium on Computers and Communication (ISCC), IEEE, 2015, pp. 809–815.
[63] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, G. Carle, Dtls based security and two-way authentication for the internet of things, Ad Hoc Netw. 11 (8) (2013) 2710–2723.
[64] Q. Ping, W. Meng, Survey on privacy preservation in iot, Appl. Res. Comput. 30 (1) (2013) 13–20.
[65] J. Vaidya, C. Clifton, M. Kantarcioglu, A.S. Patterson, Privacy-preserving decision trees over vertically partitioned data, ACM Trans. Knowl. Discov. Data 2 (3) (2008) 14.
[66] Z. Yang, R.N. Wright, Privacy-preserving computation of bayesian networks on vertically partitioned data, IEEE Trans. Knowl. Data Eng. 18 (9) (2006) 1253–1264.
[67] H. Ning, H. Liu, L.T. Yang, Aggregated-proof based hierarchical authentication scheme for the internet of things, IEEE Trans. Parallel Distr. Syst. 26 (3) (2014) 657–667.
[68] H. Liu, H. Ning, Q. Xiong, L.T. Yang, Shared authority based privacy-preserving authentication protocol in cloud computing, IEEE Trans. Parallel Distr. Syst. 26 (1) (2014) 241–251.
[69] X. Yao, H. Liu, H. Ning, L.T. Yang, Y. Xiang, Anonymous credential-based access control scheme for clouds, IEEE Cloud Computing 2 (4) (2015) 34–43.
[70] H. Liu, X. Yao, T. Yang, H. Ning, Cooperative privacy preservation for wearable devices in hybrid computing-based smart health, IEEE Internet of Things Journal 6 (2) (2019) 1352–1362, https://doi.org/10.1109/JIOT.2018.2843561.
[71] S.-W. Hwang, H. Tao, D.-H. Kim, H. Cheng, J.-K. Song, E. Rill, M.A. Brenckle, B. Panilaitis, S.M. Won, Y.-S. Kim, et al., A physically transient form of silicon electronics, Science 337 (6102) (2012) 1640–1644.
[72] N. Banerjee, Y. Xie, H. Kim, C.H. Mastrangelo, Microfluidic device for triggered chip transience, in: SENSORS, 2013 IEEE, IEEE, 2013, pp. 1–4.
[73] X. Gu, W. Lou, R. Song, Y. Zhao, L. Zhang, Simulation research on a novel micro-fluidic self-destruct device for microchips, in: 2010 IEEE 5th International Conference on Nano/Micro Engineered and Molecular Systems, IEEE, 2010, pp. 375–378.
[74] J.-W. Han, M.-L. Seol, Y.-K. Choi, M. Meyyappan, Self-destructible fin flip-flop actuated channel transistor, IEEE Electron. Device Lett. 37 (2) (2015) 130–133.
[75] Y. Zhao, W. Lou, D. Li, Study of a novel bi-stable and easy integrated mems etbs, in: 2012 7th IEEE International Conference on Nano/Micro Engineered and Molecular Systems (NEMS), IEEE, 2012, pp. 257–260.
[76] Y. Zhao, W. Lou, D. Li, Research in a novel integrated chip of safe and initiation control, in: Tech. Proc. NSTI Nanotechnology Conf. Expo, NSTI-Nanotech, 2012.
[77] A.Z. Yue, B.L. Kang, C.L. Wenzhong, D.L. Dongguang, M. Zhihui, Study of asic self-destruction technology based on mems initiator, in: The 8th Annual IEEE International Conference on Nano/Micro Engineered and Molecular Systems, IEEE, 2013, pp. 851–854.
[78] M. Plastoi, D.-I. Curiac, Energy-driven methodology for node self-destruction in wireless sensor networks, in: 2009 5th International Symposium on Applied Computational Intelligence and Informatics, IEEE, 2009, pp. 319–322.
[79] D.-I. Curiac, M. Plastoi, O. Banias, C. Volosencu, R. Tudoroiu, A. Doboli, Combined malicious node discovery and self-destruction technique for wireless sensor networks, in: 2009 Third International Conference on Sensor Technologies and Applications, IEEE, 2009, pp. 436–441.
[80] R. Perlman, The Ephemerizer: Making Data Disappear, Tech. rep., Mountain View, CA, USA, 2005.
[81] J. Xiong, X. Liu, Z. Yao, J. Ma, Q. Li, K. Geng, P.S. Chen, A secure data self-destructing scheme in cloud computing, IEEE Transactions on Cloud Computing 2 (4) (2014) 448–458.
[82] L. Zeng, Y. Wang, D. Feng, Cloudsky: a controllable data self-destruction system for untrusted cloud storage networks, in: 2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, IEEE, 2015, pp. 352–361.
[83] R. Geambasu, T. Kohno, A.A. Levy, H.M. Levy, Vanish: increasing data privacy with self-destructing data, in: USENIX Security Symposium, vol 316, 2009.
[84] J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, P.S. Chen, A full lifecycle privacy protection scheme for sensitive data in cloud computing, Peer-to-peer Networking and Applications 8 (6) (2015) 1025–1037.
[85] L. Zeng, S. Chen, Q. Wei, D. Feng, Sedas: a self-destructing data system based on active storage framework, IEEE Trans. Magn. 49 (6) (2013) 2548–2554.
[86] S. Sutar, A. Raha, D. Kulkarni, R. Shorey, J. Tew, V. Raghunathan, D-puf, An intrinsically reconfigurable dram puf for device authentication and random number generation, ACM Trans. Embed. Comput. Syst. 17 (1) (2018) 17.
[87] R. Arjona, I. Baturone, A dual-factor access control system based on device and user intrinsic identifiers, in: IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2016, pp. 4731–4736.
[88] T. Balan, A. Balan, F. Sandu, Sdr implementation of a d2d security cryptographic mechanism, IEEE Access 7 (2019) 38847–38855, https://doi.org/10.1109/ACCESS.2019.2904909.
[89] X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on blockchain for internet of things, Comput. Commun.136(2) (2019) 10–29, https://doi.org/10.1016/j.comcom.2019.01.006.
[90] Iota. https://www.iotatoken.com, 2017.