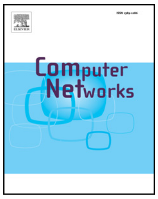
Computer Networks 148 (2019) 295–306

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



A survey on internet of things security from data perspectives

Jianwei Hou, Leilei Qu, Wenchang Shi*

School of Information, Renmin University of China, Beijing, P.R. China

ARTICLE INFO

Article history:
Received 6 August 2018
Revised 31 October 2018
Accepted 27 November 2018
Available online 28 November 2018

Keywords:
Internet of things
Security
Safety
Privacy
Forensics

ABSTRACT

As the Internet of Things (IoT) sees an increasing use in the society, the security challenge it faces is becoming more and more severe. Data collected and shared in the IoT plays an important role in the significance of the IoT. Observing from a data perspective may be of great help in understanding IoT security. Though a number of surveys on IoT security have been out there, none of them is from such a perspective. To fill the gap, this paper investigates IoT security from data perspectives. Combining the concept of typical IoT architectures with data life cycles, the paper proposes a three-dimensional approach to exploring IoT security, i.e., with the one-stop, multi-stop and end-application dimensions. The one-stop dimension explores IoT security by observing data on an IoT device, the multi-stop dimension by observing data among a group of IoT entities, and the end-application dimension by observing data used in IoT applications. While data may flow from IoT end-point devices through the Internet to a cloud or vice versa, the most demanding IoT-specific issues are in the space from IoT end-point devices to the border of the Internet, therefore the paper focuses on this space. The one-stop dimension discusses IoT security with respect to data that may flow from and to an end-point device. The multi-stop dimension works from the angle of data among a group of IoT entities, concerning secure communication, authentication and access control. The end-application dimension acts from the viewpoint of data usage in IoT applications, covering privacy, forensics, and social or legal challenges of the entire system. The paper makes an in-depth analysis of the latest development in IoT security by observing from data perspectives, summarizing open issues and suggesting promising directions for further research and applications of IoT security.

1. Introduction

The Internet of Things (IoT) is a marvel of technology development, which enhances more and more pervasive connectivity around the world. It expands the communication capability of information and communication technologies (ICTs) from “Any TIME” and “Any PLACE” to “Any THING” [1]. However, on the other hand, it makes the security situation more and more severe.

Obviously, the IoT stimulates an explosive growth of data. The Norwegian research organization SINTEF pointed out that over the past two years, 90 percent of the world’s data had been generated at a speed of over 205,000 gigabytes per second, which was approximately equivalent to 150 million books [2]. From healthcare and retail to transportation and manufacturing, IoT provides smart services by extracting valuable information from various kinds of data collected by IoT end-point devices, which has a significant impact on social production and people’s life. It is incomplete to discuss IoT without considering data.

An IoT end-point device is not only a simple data collecting device. Most importantly, it has mandatory communication capabilities. It is a kind of data source in some sense, which may provide data to back-end servers on the Internet. Standalone devices such as smart watches or smart meters are counted as IoT devices. However, IoT devices are usually embedded in large systems, such as electronic control units (ECU) in networked vehicles [3].

A great value of the IoT is that it can capture and make use of a variety of data concerning natural environments as well as human beings. Data makes the IoT alive. We believe that, similar to that observing blood in a human body is useful to have insights into people’s health, observing data in an IoT environment may help to understand the security of the IoT.

A number of researchers have published their surveys on IoT security from several different perspectives [4–14]. However, to our knowledge, none of those surveys takes data as the main clue. In our opinion, there may be something missing in the understanding of IoT security in that case. To fill the gap, this paper probes into IoT security by observing data playing in the IoT environment.

To capture a comprehensive data-driven picture of IoT security, the paper proposes an investigation framework that takes both IoT

* Corresponding author.
E-mail address: wenchang@ruc.edu.cn (W. Shi).

https://doi.org/10.1016/j.comnet.2018.11.026

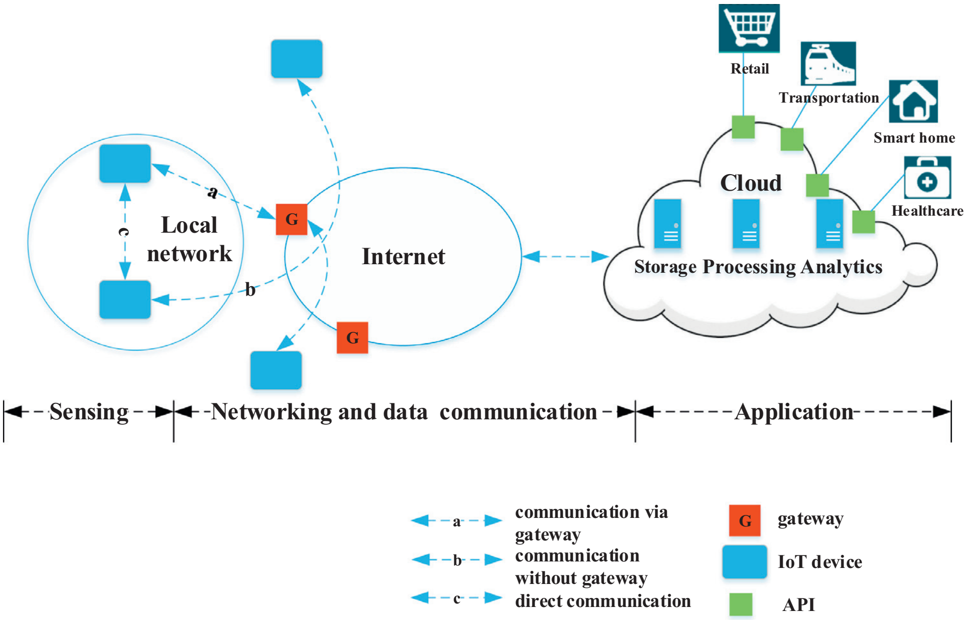


Fig. 1. An overall architecture of an IoT system.

architectures and data life cycles into account. As shown in Fig. 1, one of the typical IoT architectures describes the IoT as a multi-layered network, which consists of a sensing layer, a networking and data communication layer and an application layer [15]. Our framework is consistent with such an architecture. It can be divided into three dimensions, which are named as one-stop dimension, multi-stop dimension and end-application dimension. These dimensions have their focuses on a single IoT device, IoT entity groups and IoT applications, respectively. The paper explores IoT security through these dimensions. From the one-stop dimension, data on one IoT device is observed. From the multi-stop dimension, data moving in a group of IoT entities is observed. From the end-application dimension, data used in IoT applications is observed. With the one-stop dimension, IoT security is explored based on data that is captured by an end-point device and sent out to the Internet or that is received by the end-point device from the Internet. With the multi-stop dimension, IoT security is discussed in consideration of data flowing among a group of IoT entities. With the end-application dimension, IoT security is analyzed according to the usage of data in IoT applications. Put together, investigations from the whole framework may present a holistic landscape of IoT security.

Observed from its whole life cycle, data may exist anywhere in the IoT environment, including on an end-point device, on the Internet, or in a cloud. IoT data may flow from IoT end-point devices through the Internet to a cloud, or vice versa. Undoubtedly, IoT security related to IoT data must be investigated with consideration of the whole IoT environment. However, the most IoT-specific points of IoT security that call for IoT-specific solutions are lying in the space from IoT end-point devices to the border of the Internet. Therefore, the paper focuses on this domain, which we call the end-point domain for brevity. It makes an in-depth analysis of the latest development in IoT security from data perspectives, summarizes open issues, and suggests promising directions for further study and applications of IoT security.

The rest of the paper is organized as follows. In Section 2, we summarize related work of existing IoT security surveys. In Sections 3, 4 and 5, we present discussions of IoT security from each dimension, respectively. Finally, we conclude the paper with Section 6.

2. Related work

There are a number of surveys discussing IoT security from different perspectives in the literature.

Ray et al. [4] explored security-affecting factors in IoT that divided IoT security into three categories, which are factors that made security more challenging for IoT, factors that facilitated security assurance, and factors that made IoT security different from traditional network security. It helps understanding the specificity of IoT security.

Guo et al. [5] and Yan et al. [6] focused on trust management in an IoT environment. Yan et al. [6] proposed a research model of trust management in IoT based on IoT system models. Trust management in IoT covers not only trust management in each layer and cross-layers but also user trust in IoT devices and services. Guo et al. [5] focused on trust computation in assessing trustworthiness of services in an IoT environment.

Since a distributed architecture is a future direction of IoT development, [7] analyzed the features of distributed and centralized IoT systems. And it studied the challenges and promising measures in design and deployment of distributed IoT security mechanisms, concerning authentication, access control, protocol and network security, privacy, trust, and fault tolerance.

Wolf and Serpanos [8] and Banerjee et al. [9] focused on handling security and safety in IoT. Due to the cyber-physical characteristic of IoT, IoT security needs to have a unified view of security and safety. Combining a physical system with a network system has an impact on threat models of IoT and expands attack surfaces of IoT. Changes to the physical plant's behavior, whether due to failures or malice, can change the state of the computing subsystem while changes to data in the cyber subsystem can change the plant's physical state [8].

Some surveys focused on security solutions to IoT security issues. Alaba et al. [10] proposed a taxonomy to classify IoT security threats into four aspects, which are related to application, architecture, communication, and data. Sicari et al. [11] provided an overview of research efforts in terms of access control, confidentiality, authentication, authorization, privacy, middleware, and trust in IoT. These surveys mainly discussed classical security solutions to IoT security based on cryptographic approaches.

Some efforts surveyed IoT security from the perspective of IoT architectures. Authors in [12] investigated IoT security challenges by discussing attacks in each layer of an IoT three-tier architecture. Considering that techniques supporting an IoT architecture may have more or less security problems, authors in [13] and [14] discussed security issues related to techniques and protocols concerning each layer of an IoT architecture and introduced corresponding solutions. They explored IoT security with regard to each layer of an IoT architecture, giving an overview of IoT security. However, it is insufficient to investigate IoT security according to isolated layers of an IoT architecture. More efforts should be taken to explore the security of an IoT system in a holistic way.

The aforementioned contributions from the literature have laid a good foundation for understanding IoT security from several different perspectives. Nevertheless, data has not yet been put in a leading position in portraying IoT security. We firmly believe that a data-driven observation may reveal some new findings that may not show up in other ways. Therefore, we try our best to shed new light on IoT security in this paper from data perspectives.

3. IoT security from the one-stop dimension

In this section, we explore IoT security by observing data on an IoT end-point device. Data may be collected and sent out to the Internet by an end-point device, or may be received by the end-point device from the Internet. Data flowing to and from an end-point device, i.e., input data and output data, which has interaction effects between the device and the Internet, should be considered for IoT security.

3.1. Output data related security

Massive IoT end-point devices are collecting a large volume of data and uploading it to the Internet for IoT applications. Some sensory data collected by IoT devices is sensitive and highly valuable, which is potential gains for attackers and commercial competitors. So IoT end-point devices should ensure the confidentiality requirement of data provided to the Internet. Additionally, the authenticity of output data has a direct impact on the reliability of services involving industry, economy, and social life. Therefore, it is important for IoT devices to ensure the confidentiality and authenticity of output data to guarantee the security of IoT applications and services.

3.1.1. Confidentiality

A general method for ensuring data confidentiality is encryption. IoT devices are usually dedicated devices with limited resources such as low computing power (e.g., 8-bit microcontroller), limited battery supply, small (gate) area, and limited storage [16]. General encryption algorithms that consume excessive resources may not be applicable to resource-constrained devices. In IoT, the overhead of encryption algorithms should be reasonable for device performance when providing a sufficient level of security [16]. There is an urgent need for lightweight ciphers to ensure the confidentiality of IoT data throughout its life cycle.

Plenty of lightweight ciphers have been proposed. The cryptographic structures of these newly designed lightweight ciphers mainly include Feistel structure (or its variant) (e.g., SEA [17], LBlock [18]), SP networks structure (e.g., PRESENT [19], mCrypton [20]), and other structures (e.g., KATAN/KTANTAN [21]). Some work simplified the hardware implementations of standardized block ciphers. For example, [22] simplified the key generation process of AES to improve efficiency of the algorithm while increasing the length of keys and rounds of encryption to maintain the security level of the algorithm.

The designers of lightweight ciphers must cope with trade-off among security, cost and performance according to actual requirements of target scenarios [21]. Taking RFID tags as an example, most of them are used in low-cost environments of electronic tickets. The security requirement of this scenario is not high while the demands for low power-cost and low latency are stricter [23]. Hatzivasilis et al. [24] evaluated 52 block ciphers and 360 implementations based on their security, performance, and cost, classifying them with regard to their applicability to different types of embedded devices and referring to the cryptanalysis pertaining to these ciphers.

Cryptanalysis has revealed that many lightweight ciphers are vulnerable to side-channel attacks due to their relatively simple structures [24]. In general, devices may inevitably leak information, such as power consumption and electromagnetic radiation, during the encryption step. This leaked information can be used to effectively reduce the search space of the key and even to extract the key directly. Therefore, a side-channel attack is a serious threat to the ciphers applied to many IoT devices, such as smart cards, RFID-based systems.

Lo'ai and Somani [25] studied the time-based and fault-based side-channel attacks on the most widely-used encryption algorithms (e.g., AES, ECC, and RSA) in IoT and introduced some countermeasures to mitigate side-channel attacks. Zhang et al. [26] proposed a new general framework to analyze and evaluate algebraic fault attacks on lightweight block ciphers.

Some researchers put forward the use of physical features to generate keys. Majzoobi et al. [27] used a unique physical structure called Physical Unclonable Functions (PUFs) to generate keys for identification. Instead of storing secrets in memory, PUFs derive a secret from the physical characteristics of the Integrated Circuit (IC) without the requirement of expensive secure hardware [28]. Therefore, much research has been done on the applications of PUFs in key generation.

3.1.2. Authenticity

Data sensed and generated by IoT devices should be trustworthy to reflect the real-world environment precisely. The authenticity of output data has a significant impact on the security of IoT applications. An IoT device is usually unattended and lacks physical protection. Physical attacks on a device, including node copying, replacement, and hijacking, may compromise the integrity of the device. Considering the authenticity of output data generated by an IoT device, it is extremely important to verify the integrity of the device. Generally, attestation techniques are widely used to verify the integrity of devices with the dedicated hardware(e.g., TPM). Traditional attestation methods designed for resource-rich devices may not be suitable for direct application to IoT devices to verify whether the device has been tampered. IoT devices call for lightweight attestation methods. The detailed related work of attestation in IoT is summarized in Table 1.

Typically, there are two types of attestation methods, including static attestation and runtime attestation. Static attestation verifies the integrity of the static binaries on the prover. Especially, swarm attestation is a specific type of work in static attestation to verify the integrity of a group of provers. Runtime attestation verifies the control flow of programs on the prover at runtime.

Three main approaches to static attestation on one device have been identified in the literature, which are software-based, hardware-based and hybrid.

Software-based attestation usually exploits side-channel information to verify the integrity of resource-constrained embedded devices without special hardware. Software-based attestation may be devided into two main categories. One is time-based, such as SWATT [29], Pioneer [30] and SCUBA [31], and the other is memory-based [32,33]. All software-based methods make strong

Table 1
Summary of related work in lightweight attestation.

Type of attestation	Object of attestation	Representative work
Static Attestation	The integrity of static binaries on a prover	Software-based Attestation: (1) Time-based, SWATT [29], Pioneer [30] and SCUBA [31] (2) Memory-based, [32,33] Hybrid Attestation: SMART [34], SPM [35], SANCUS [36], TrustLite [37] , TyTAN [38] Hardware-based Attestation: [39,40]
	The integrity of static binaries on provers (Swarm Attestation)	SEDA [41], SANA [42]
Runtime Attestation	Runtime behaviors of attested code on a prover	C-FLAT [43], LO-FAT [44]

assumptions about the capabilities of the adversary: (1) The verifier communicates directly with the prover with no intermediate hop and no cyber attack (e.g., imitation or collusion with other devices). (2) There is no modification on the hardware of the prover. However, in a real IoT environment, devices usually communicate through multi-hop networks. And they are usually vulnerable to physical intrusion because they are unattended.

Hybrid methods employ software/hardware co-design to defend against adversaries in a network setting (i.e., multiple hops between the prover and the verifier), while minimizing hardware changes [45]. Without the support of dedicated secure hardware, hybrid methods cannot defend against the physical intrusion. Main research on hardware-software hybrid attestation methods includes SMART [34], SPM [35], SANCUS [36], TrustLite [37] and TyTAN [38].

Both hybrid and software-based methods cannot defend against physical attacks, since keys on devices can be obtained and the prover can be impersonated and/or cloned [46]. Only hardware-based attestation can defend against physical attacks. It relies on explicit, purpose-built trust anchors(e.g., a TPM or an SGX-capable CPU) which are usually unlikely equipped on IoT devices. Therefore, some specific physical hardware characteristics are applicable to the attestation in IoT, such as PUFs [39,40].

Generally, IoT devices are deployed on a large scale. To verify the integrity of a large scale of devices, SEDA [41] firstly proposed swarm attestation for embedded devices. SANA [42] proposed a novel signature scheme for efficient swarm attestation. In specific IoT application scenarios, such as an ad-hoc vehicular network, nodes may join and leave the swarm dynamically, which makes it more difficult to attest a device swarm.

Static attestation methods discussed above only verify the integrity of binaries and not of their execution [45]. In this respect, C-FLAT [43] and LO-FAT [44] took a step by exploiting runtime attestation to provide precise attestation on the execution path of a program for the case of embedded devices.

3.2. Input data related security and safety

IoT bridges the gap between the cyber world and the physical world, so that hacking into a device in the cyber world can bring threats to the real-world and vice versa. Changes in the physical state of the device can affect its computing system, and data changes in the network or computing system can also affect the physical state of the device [8].

Safety means “freedom from accidents or losses” [8]. Some devices may execute operations based on data received from the Internet – input data, coupling security and safety concerns in IoT. Leveraging input data, including the false data generated by the system itself and the malicious data sent by adversaries due to the vulnerabilities of systems, attackers may compromise the devices. Unsafe and insecure operations on IoT devices may result in a real loss of services and even the loss of life. For example, adversaries can send malicious control data to medical equipment to speed up the pacemaker or the drug infusion pumps, endangering user’s life.

Most IoT end devices are constantly connected to the Internet and are usually with naive security configurations. Leveraging vulnerabilities on a device, adversaries can control the device remotely. Mirai is a very famous malware that can build a botnet with millions of compromised smart cameras. Since the advent of Mirai at the end of 2016, security incidents related to Mirai and its variants (e.g., Persirai, Satori, Okiru) have been frequent [47]. Mirai leverages the vulnerabilities of default passwords to gain the control of IoT devices by Telnet password brute-forcing. More and more research is finding technical and non-technical solutions to deal with Mirai and its variants [48,49].

Reaper – a new kind of botnet, which may be substantially more dangerous than Mirai, utilizes a list of known vulnerabilities to enable an attacker to gain full access to a target device. Mirai and reaper are sizable threats, but it is even worse that some of IoT security threats may be small enough to evade detection. Infected devices can be used to steal personal data and mine cryptocurrencies, on top of traditional DDoS attacks.

There is no good way to reduce malicious traffic produced by these systems except for squelching it at the source. George et al. [50] recommended that device manufacturers should limit the amout of network traffic that IoT devices can generate to levels reasonably needed to perform their functions.

On the other hand, some IoT devices are nodes of infrastructure, including basic sensors for industrial facilities. It is more dangerous that the compromised node can be an entry point for the attacks on the overall infrastructure, which may cause great life and property losses for individuals and nations.

There is a rapid expansion in the size of botnets due to the long-term and non-update problems of the target IoT devices. Vulnerabilities on devices must be fixed in time to prevent attackers from obtaining control of the devices. However, most devices cannot be patched conveniently nowadays. Without general automatic update tools, it takes plenty of overhead to update massive IoT devices and the updating process itself can be complex for the average user. Moreover, vendors may usually not provide users with patches or update services after products are sold. That may cause problems in the future when hackers find and exploit vulnerabilities on devices to launch attacks for their own gains. Therefore, update mechanisms should send the latest firmware to devices timely and automatically.

However, remote updates may also bring new risks to IoT devices. Adversaries may launch rollback attacks on firmware and exploit vulnerabilities of buggy versions to attack devices. Device vendors or manufacturers should encrypt and digitally sign the updated release information to ensure the integrity and authenticity of the update.

Moreover, there will be a traffic bottleneck in a centralized architecture of updating mechanisms. In order to solve the problems of traffic bottleneck, [51] explored a distributed update method using blockchain techniques. Devices broadcasted updating requests to blockchain nodes on a peer-to-peer decentralized network. If the firmware version of the device was not the latest, the device would download the latest version. If the firmware version of the device was already up-to-date, a blockchain node would check the integrity of firmware on the requesting node. However, due to the nature of broadcasting, the broadcasted requests may result in useless network traffic and unnecessary operations on unrelated nodes.

Over-the-Air (OTA) update is a practice of remotely updating codes on embedded devices. Distributing new firmware through OTA will bring plenty of overhead (e.g., energy consumption, download time). Therefore, if not necessary, a partial code update is a better choice for devices updating to support novel standards and meet new requirements. Ruckebusch et al. [52] proposed a new software update mechanism for partial code updates on protocols and applications at runtime. This architecture consists of three levels – a static system level, a dynamic component level, and a kernel level. Authors in Ruckebusch et al. [52] implemented their approach on one of the typical IoT operating systems, Contiki, without major modifications of existing network protocols and applications.

3.3. *Open issues*

For confidentiality, current research on lightweight encryptions achieves a high degree of overhead reduction. Now, essential considerations of confidentiality on end devices should be more about practical applications of algorithms in the real world, including speed optimization and latency reduction.

For authenticity, more research on attestation for a group of devices is expected. Large scale usually implies heterogeneity, which increases the complexity of attestation. An IoT device can switch from online to offline at any time, which makes it dynamic and indeterminable. It's difficult to obtain the real status of a device swarm. The issues about how to improve efficiency, robustness, and accuracy of swarm attestation have not been solved well.

Furthermore, IoT devices lack a common update mechanism due to heterogeneous computing systems. It is hard to apply timely updates for all end devices. Thus, vulnerabilities exposed for a long time can still be seen on most IoT devices. They are around our daily lives but quite vulnerable to exploitation, which is both a technical and social concern.

4. IoT security from the multi-stop dimension

In this section, we investigate IoT security by observing data that may flow among a group of IoT entities. Secure communication, authentication and access control related to interactions of IoT entities will be covered. Interconnectivity is a fundamental characteristic of IoT entities that can directly or indirectly interact with the Internet. To ensure the interactions of entities, communication networks transfer data captured by IoT end-point devices to applications and other devices, as well as instructions from applications to IoT devices [1].

4.1. *Communication related security*

In general, there are three types of communication for IoT devices to communicate with others: communicating through the Internet via a gateway, communicating through the Internet without a gateway, communicating through a local network (i.e., a network providing local connectivity between devices and between devices and a gateway, such as an ad-hoc network) [1], as shown in Fig. 1. For the first two types, devices connect to the Internet via a variety of available wired or wireless technologies (e.g., WiFi, Bluetooth, NFC). For the security issues of wireless communication protocols, we point inquisitive readers to [53,54].

As for the last communication type, there are plenty of devices in IoT consisting of sensors and actuators with routing capabilities. They construct local networks to communicate with each other and use gateways to connect to the Internet. These devices have self-organizing capabilities and usually lack protection, so that they can join and leave the local network at any time throughout routing and are easily hijacked [55]. To ensure the security of communication, secure routing in an IoT local network needs to select the nodes with high trust level to create a reasonable route. Malicious nodes in a local network may bring serious security problems [56]. For example, malicious nodes can transmit a large amount of false routing information to its neighbors, causing its neighbor's routing table to overflow and hide the real routes [57].

Therefore, secure communication capabilities of IoT entities need to ensure the security of data transmission in IoT networks. The main research on the security issues related to communication falls into three categories: (1) designing secure communication protocols for IoT devices; (2) designing efficient malicious node identification systems; (3) designing lightweight trust management schemes to evaluate the trust level of nodes in an IoT local network.

Some traditional IoT routing protocols, such as RPL [58] designed for 6LowPAN [59], are still facing many security problems [55]. SMRP [60] proposed a secure multi-hop routing protocol with multi-layer parameters. When a node attempts to join an existing network or to form a new network, it must verify multi-layer parameters. Because the creation of multi-layer parameters would bring a lot of overhead, so that the protocol could not be directly applied to large-scale networks.

DEMEM [61] proposed a Distributed Evidence-driven Message Exchanging intrusion detection Model that allowed distributed detectors to cooperatively detect routing attacks with minimal communication overhead. It used finite state machines to specify correct routing behaviors and used distributed network monitoring to detect run-time violations of the specifications. ActiveTrust [62] proposed an active detection-based secure routing scheme. The most important innovation of ActiveTrust is that it can actively detect black hole attacks by creating multiple detection routes to detect quickly and ensure the secure routing. More importantly, it makes full use of energy in non-hotspots to create as many detection routes as needed to improve energy efficiency.

Trust-based schemes predict future actions of nodes based on past observation of nodes and assist in effective identification of suspicious nodes. TSRF [63] is a secure routing framework based on trust derivation. It was implemented by direct and indirect observation of behavioral patterns of sensor nodes with trust values among nodes represented in a range from 0 to 1. A value of 0 represents a low level of trust of the node and a value of 1 represents a good level of trust of the node. However, due to complex trust computation, TSRF has a large computational overhead in the nodes. Therefore, protocol designers must minimize the impact on network performance while improving the security level of protocols. TERP [64] proposed a new Trust and Energy-aware Routing Protocol to address the trustworthiness and energy efficiency issues of routing. It uses the weight of trust, energy, and hop counts to select the nodes that are trustworthy, energy-efficient and have the shortest route to the destination.

Moreover, secure communication protocols for IoT devices should have self-healing capabilities, which means that the protocol can automatically recover from failures within a certain period of time without human intervention. Local networks may initially be unstable when attackers send many malicious packets to the networks. Nonetheless, due to the self-healing capability of protocols, the network can recover itself and isolate malicious nodes over time [65].

Table 2
Summary of related work in authentication.

Classification of related work	Specific research direction
Authentication in different scenarios	Internet of Vehicles [71,72], Smart Grid [73,74], Smart Healthcare [75], *etc.*
Authentication credentials	Key-based authentication schemes, including symmetric, asymmetric or hybrid keys
	Physical-characteristics-Based authentication schemes [76]
	Location- based authentication schemes [77]
	Biometrics-based authentication schemes [78]
Functional requirements of authentication	Mutual authentication [69,79]
	Anonymity and unlinkability of authentication [80–82]
	Cross-Domain authentication [83]
	Continuous authentication on data stream [84]

Table 3
Summary of related work in access control.

Classification of related work	Specific research direction
Models of access control	Role-based Access Control (RBAC) Model [85]
	Attribute-based Access Control(ABAC) Model [86]
	Other models, e.g., Usage Control(UCON) Model [87], Capabilities-based(Cap-BAC) Model [88]
Functional requirements of access control	Dynamic [85], continuous [89], fine-grained [90,91] requirements of access control
Access control in different scenarios	Internet of Vehicles [86], Smart Grid [92], Smart Healthcare [17,93], *etc.*

4.2. Authentication and access control

IoT integrates a large number of physical objects that are uniquely identified, ubiquitously interconnected and accessible through the Internet [66]. Authentication and access control are the main security mechanisms to ensure the security of interactions among different entities (devices or users). Access control and authentication are the process of determining whether an entity can access resources and authentication, a process of identifying an entity, is a prerequisite for authorization [67]. With the limitation in computing, energy, storage of devices, the need for schemes of authentication and access control applicable to IoT is pressing.

In various IoT application scenarios, such as smart healthcare, intelligent transportation and smart home, heterogeneous devices and network architecture lead to different demands of authentication and access control to ensure the security of interactions among entities.

Authentication. In a decentralized environment, it is necessary to implement two-way authentication between two IoT entities with an absence of a trusted third party. While data holders authenticate the data collector, data collectors also need to identify or authenticate users and devices as legitimate data holders before collecting data from data holders [68]. Some work has investigated the security issues of RFID technology which is widely used in IoT, including security and privacy issues of authentication between RFID readers and tags [69].

Some efforts have been made to work on the credentials used for authentication. Besides the traditional key-based credentials, location information and biometric-characteristics, as well as physical characteristics can also be credentials for authentication.

PUFs are promising innovative primitives for low-cost authentication. Gao et al. [70] proposed an obfuscated challenge-response authentication protocol for resource-constrained devices at low cost, based on PUFs. Biometrics-based authentication needs to obtain users' biometric characteristics. However, many users may be reluctant to share their personal information for privacy concerns. On the other hand, biometric characteristics may not always follow the same pattern, and some unpredictable factors may have an impact on the results. Thus, the accuracy of biometrics computation that is closely related to the stability and accuracy of authentication calls for more research.

Additionally, under the scenarios of Internet of Vehicles, smart grid, and smart healthcare, anonymity and unlinkability of identities need to be considered. And IoT devices may move from one network to another. How to solve the issues of cross-domain authentication for devices also requires more research [11].

Typical research related to authentication in IoT is shown in Table 2.

Access Control. In IoT, access control is to assign different privileges of resources to different actors of a wide IoT network [11]. Users and devices, as data holders, can only provide specific data to specific data collectors for specific purposes [68]. Most IoT devices operate automatically based on the context of real-time streaming data. IoT scenarios call for lightweight, continuous, dynamic, context-based access control schemes.

Most existing IoT systems adopt traditional access control schemes of existing computer systems based on roles [85] and attributes [86]. Most solutions have high computational complexity and are based on static attributes. Static attributes are overdependent on user-defined rules, so that it may be not applicable to the automation requirement in some IoT scenarios. With the need of automatic operation in IoT, dynamic context-based attributes, such as location and time-based attributes, can also be used for dynamic authorization and active authentication. Some work utilizes Usage Control (UCON) models to deal with the issues of continuous authorization before and during the process of accessing. The UCON model supports dynamic changes of attributes. That is, if access attributes change during accessing, which causes failure to meet the access requirements, the access rights will be revoked [87].

Typical research related to access control is shown in Table 3.

4.3. Open issues

Firstly, because IoT networks are usually self-organizing and wireless communication technologies are widely used, it is possible for malicious nodes to be introduced into a local network easily. However, there is still not any effective and lightweight approach to malicious nodes detection in IoT. Blockchain technology can build mutual trust at low cost in a decentralized environment without a central manager. It may be a future research direction for the security of data exchange and multi-party collaboration in IoT.

As some IoT devices may execute operations automatically, it will be difficult to manage these devices from a networking and

Table 4
Summary of related work in privacy in different IoT application scenarios.

Typical IoT application scenarios	Related work in privacy
Smart home	Privacy-preservation of traffic [99–101]
Digital healthcare	Pseudonym management [102–104]
	Anonymous authentication [105–107]
	Privacy-preserving access control [108]
Smart grid	Privacy-preserving data aggregation [109–111]
	Privacy-preservation of smart meter data [112,113]

data management perspective. Therefore, it is important to carefully evaluate the reliability of authentication and access control methods. The mobility of smart cars or other wearable devices may call for cross-domain authentication. In addition to exploring new authentication approaches based on PUFs or biological characteristics, an effective but low-cost method for authentication in the real world is still a challenging topic.

5. IoT security from the end-application dimension

In this section, we explore IoT security by observing data used in IoT applications. A large volume of data is collected by IoT devices, transferred over networks and used by different IoT applications. Keeping IoT data life cycles in mind, from the view of data usage in IoT applications, we will investigate privacy, forensics, and social or legal challenges of the whole IoT system.

5.1. Privacy concern

In real IoT scenarios, different IoT applications leverage data collected from IoT devices to provide convenient and smart services for users while introducing potential privacy concerns. Private information may be leaked at any phase of a data life cycle in IoT environments. Therefore, privacy concerns must be considered from system perspectives. Besides individual data like fingerprints and heartbeats, which are directly related to a user's privacy, some environmental information sensed by IoT devices can be utilized to infer extra information about user's preference and trajectory. The aggregated data from various IoT devices can add up to a total surveillance of our lives [94]. A user can be both a recipient of data or services and a subject to data collection by smart things at the same time [95]. Compared to the Internet where users have to take an active role to put their privacy at stake (i.e., query for services), much data about users are collected and transfered in IoT without their awareness [96]. A large volume of data is being generated by IoT automatically with higher velocity than before, and any breaches in security will have a knock-on effect on personal security and privacy.

There is an urgent demand for research on privacy protection technologies in IoT during data transmission, aggregation, storage, mining, and processing [1]. Moreover, machine learning and data mining technologies can add the business context to the raw data automatically without human intervention, threatening users' privacy. Under this background, more efforts need to be devoted to privacy-preserving data mining techniques [97] and privacy-preserving machine learning techniques [98]. For instance, even though smart home devices are not designed to capture privacy-sensitive activities, such activities may be identified by inference techniques.

Because different application scenarios involve different devices and architecture and have different security requirements, research on privacy concerns in various IoT application scenarios has different focuses, as shown in Table 4.

In a smart home, passive attackers can collect raw data closely related to users to infer users' routines by eavesdropping on the communication between smart routers and smart devices. For example, when the light changes from on to off, it can be inferred that users may have left home. Active attackers may pretend to be legitimate users to gain access to smart devices and to extract sensitive information. To address privacy concerns, smart devices need to provide end-to-end encryption of communication. However, [99] demonstrated that an ISP or other network observers can infer privacy-sensitive in-home activities by analyzing traffic from smart homes containing commercially-available IoT devices even when devices use encryption. Liu et al. [100] and Song et al. [101] explored privacy preservation of traffic in a smart home. Moreover, the over-privilege problem in SmartApp authorization would also lead to privacy concerns [114,115].

In digital healthcare, medical records and healthcare data are more valuable in the black market than credit card numbers now [116]. The primary security target for digital healthcare is to ensure the security of primary health data and protect identifiable health data from unwarranted access or disclosure during data acquisition, transmission, and storage. On the other hand, personal treatment information is often shared by the same patient group, which helps the exchange of patient conditions and treatment information among doctors and patients from different regions. It is essential to protect security and privacy of personal medical information when sharing data for public benefit. To solve the above privacy concerns in digital healthcare, there is plenty of research on pseudonym management of medical data [102–104], anonymous authentication [105–107], and privacy-preserving access control to medical data [108].

In smart grids, fine-grained data that is collected periodically by smart meters to improve the efficiency of grid operation can easily reveal household activities [117]. A smart grid consists of a control center, smart meters, and gateways. Smart meters collect primary home electricity usage information and send the encrypted data to gateways. Then the gateways decrypt the data from all smart meters and aggregate it. Gateways encrypt the aggregated data and send it to a control center for further analysis and processing (e.g., balancing electricity load and optimizing energy consumption) [118]. Privacy protection must be considered in electricity data aggregation for residential grids. However, there is a content-oriented privacy risk in the case that these intermediate nodes are compromised by adversaries. Thus, gateways should not carry out aggregation operations in a plaintext manner. Homomorphic encryption is one of the typical approaches that allows an aggregator (gateway or control center in general) to execute the operation directly on ciphertext under the same key, without the need of data decryption [118]. Much effort has been devoted to privacy-preserving aggregation schemes [109–111]. Because individual load curves per household in the smart grid can be used to infer personal consumption behaviors or living habits [119]. Therefore, there is an urgent need to guarantee the anonymity and unlinkability of electricity data to ensure that data cannot be associated with a specific user and disclose a user's trajectory in smart grid scenarios.

5.2. Forensics challenges

With IoT gradually permeating our lives, accidents and attacks involving IoT services or devices will happen inevitably. Forensic investigations need to be conducted in the IoT infrastructure, when IoT is the target of attacks or used to launch an attack. Data collected and shared by IoT applications introduces both opportunities and challenges into forensics. In the context of IoT, there are a diverse range of potential evidence sources, so that the forensics may need to combine multiple digital forensic methods and techniques, increasing the difficulty of forensics. Specialized tools and techniques, as well as standardized procedures are required for collecting, preserving and analyzing residual evidence in the IoT environment. Traditional digital forensics cannot be directly applied in IoT due to highly heterogeneous and frequently changing environments. With limited memory of most IoT devices, they need to transfer data to a cloud or a local hub before evidence is overwritten. IoT forensics can be identified as a combination of three digital forensics schemes, including cloud forensics, network forensics and device level forensics [120]. However, as evidence can be modified at any step of data life cycles, it presents challenges to make the chain of evidence secure. Challenges of forensics in IoT are summarized as following.

1) Resource-limited characteristic of devices. With limited resources (e.g., computing power, memory), it is hard for IoT devices to achieve persistent recording. Potential evidence might not be maintained on devices or just be maintained for a very short period of time before being overwritten by the latest data. The energy limitation in some scenarios, such as solar-powered nodes, leads to intermittent and partially incomplete information when devices power down.
2) Heterogeneous characteristic of devices. Heterogeneous devices in IoT with proprietary interfaces lead to difficulty in accessing stored values, calling for specialized information-retrieval tools [121]. Data on heterogeneous devices varies in size and format. Different data formats, protocols and physical interfaces complicate the process of evidence extraction. There is an absence of general tools for collecting, preserving and analyzing data in IoT.
3) The growth in numbers and types of devices. IoT presents a considerably large number of potential evidence sources from personal health devices to connected vehicles, which may introduce additional complexity to identify and find potential IoT evidence sources in crime scenes. In addition, with the absence of temporal information such as modified, accessed and created time, it is extremely difficult to correlate and sequence the digital evidence gathered from different IoT devices, some of which may have no clock [122].

DFIF-IoT [123] proposed a generic Digital Forensic Investigation Framework for IoT to standardize investigation procedures including three processes – proactive process, IoT forensics, and reactive process. Proactive process aimed to make the IoT environment forensically ready. IoT forensics consisted of cloud forensics, network forensics, and device level forensics. Reactive process would occur after an incident was identified in an IoT-based environment.

FAIoT [120] proposed a centralized trusted evidence repository to ease the process of evidence collection and analyze with logging, preservation and provenance schemes.

Oriwoh et al. [124] combined the 1-2-3 Zones approach and Next-Best-Thing Triage (NBT) Model to deal with IoT-related digital forensics investigations. 1-2-3 Zones approach can be used to implement investigations systematically and to identify possible objects of forensic interest effectively. NBT model is useful to identify additional potential evidence sources when primary sources are unavailable, providing a guidance on identification of devices of interest within the established focus areas.

Privacy is another important factor to consider when analyzing and correlating the collected evidence which may contain personal information. PRoFIT (Privacy-aware IoT-Forensics) [125] integrated privacy properties with the forensics model adapted to IoT, stimulating the cooperation of citizens in digital forensic investigations. PRoFIT highlights the importance of collaborating with nearby devices to gather digital evidence from multiple sources, which helps to fully describe the context of a crime scene.

The existing work on IoT forensics is still insufficient. Most current research focuses on extending traditional forensic methods to forensics in IoT. Although existing digital forensic tools can be used in some stages of forensic investigations in IoT, there is still no general and efficient framework for forensics in IoT.

5.3. Social or legal challenges

The use of IoT is dramatically changing people's everyday life, introducing not only technical challenges but also social or legal challenges to IoT security.

Liability Dispute. Intelligent services provided by IoT may bring new responsibility disputes. For example, automated vehicles are being gradually put into use. When an accident with automated vehicles occurs, the judgment of accidental responsibility calls for a better legislation for the use of automated vehicles. The Australian National Transport Commission has drafted new Australian driving laws to support automated vehicles [126].

Data Commodification. In IoT, the wide collection and usage of a large amount of data make data a commodity and develop asset virtualization, bringing the problems of data ownership. How to standardize the management of data as a product? Who is the owner of the data? Can data be traded? All these questions bring corresponding responsibility issues. Data holders have the right to authorize and revoke authorization to the collection of their personal data. By fine-grained authorization based on context, data holders can just share the subset of data with the applications that they are willing to share with in the IoT environment.

Vulnerabilities of Social Engineering. IoT plays a vital role in human interactions, influencing social contact and people's everyday life. Fine-grained and ubiquitous data collection in IoT makes users vulnerable to social engineering attacks [127]. The best way to deceive a person is to gather as much information about him as possible. The emergence of IoT makes data collection easier by hijacking smart devices such as smart TVs, Fitbits, and Google Glass to monitor and learn voices, habits, and preferences of the target person.

Legislation Challenges. Although legislation cannot provide guarantees for the security of data usage in IoT applications, it is a way to compensate the damage caused by the misuse of data. Perfecting legislation and policy to protect data usage in IoT applications is pressing. Countries are making efforts to provide more protection for data applications.

The EU General Data Protection Regulation (GDPR) was designed to harmonize data privacy laws across Europe, reshaping the way organizations across the region approach the data that are qualified as personal data [128]. One of the central principles underpinning GDPR is to improve all EU residents' awareness surrounding consent for data processing and usage [129]. The U.S has issued Health Insurance Portability and Accountability Act (HIPAA) [130] to protect the privacy and security of certain health information. It has discussed the accessibility, integrity, and confidentiality of ePHI (electronic protected health information). IoT device manufacturers and IoT App developers should provide consumers with a HIPAA level of security when recording weight, heart rate, blood pressure, and other health insights. Unsolved questions call for additional legislation to provide guarantee for IoT services. For example, the life cycle of smart products is still modeled as buy-once-own-forever without considering the security and privacy of productions that may be borrowed and exchanged freely in sharing economy era.

5.4. Open issues

For privacy protection, as privacy regulations around the world have been in operation, the transfer and usage of private data ought to be subject to privacy regulations. However, there is still not any widely accepted technical standard for privacy protection of data storage, transmission, sharing as well as application. Privacy should be ensured from the whole system perspective. Privacy protection mechanisms of each product should be implemented in accordance with general technical standards rather than being implemented arbitrarily by developers.

For forensics challenges, there are many fields that have not been fully investigated, such as applying blockchain technologies to evidence preservation. Standardized forensic investigation frameworks and efficient synchronization approaches for evidence in IoT are deserved to design.

6. Conclusion

Considering that IoT data may reveal a novel clue to deal with IoT security and that no existing survey on IoT security is guided from the perspective of IoT data, this paper sheds light on IoT security with IoT data as a leading factor. It devises a framework for IoT security observation that takes both the typical IoT architecture and the IoT data life cycle into account, which outlines IoT security in three dimensions, i.e., the one-stop dimension, the multi-stop dimension and the end-application dimension.

As the simplest starting point, the one-stop dimension observes data flowing around a single IoT end-point device. Data may be collected by the end-point device and sent out to the Internet, or may be received by the end-point device from the Internet. Because of the resource-constrained characteristic of an IoT device, lightweight cryptos and trust execution environments are in urgent demands to ensure the security related to data that may be sent to the Internet. Meanwhile, data received from the Internet may introduce vulnerabilities of the virtual world into the real world. Compromise of data from the Internet, including control data, may lead to safety concerns of devices, infrastructures, and individuals in the physical world.

Observed from the multi-stop dimension, a group of IoT entities are interconnected through local networks or the Internet. They may need to have secure communication with backend services, which are usually provided by a cloud. The nature of dynamics, mobility and resource limitation of the IoT calls for efforts to extend existing security techniques, including secure communication, authentication and access control, to a new environment.

Finally, observed through the end-application dimension, with typical IoT application scenarios such as smart home, digital healthcare and smart grid taken as instances, the investigation is conducted to cover privacy, forensics, and social or legal challenges from the whole IoT system perspective.

In order for the IoT to further improve the quality of human life, the aforementioned challenges are pressing and should be dealt with in a sound way. The paper carries out an extensive study on the state-of-the-art of IoT security from the data perspective, specifying open issues and pointing out future research trends. We hope that it may become a valuable reference for future research on IoT security.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under grant No. 61472429, Beijing Municipal Natural Science Foundation under grant No. 4122041, and National High-Tech Research Development Program of China under grant No. 2007AA01Z414.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.comnet.2018.11.026.

References

[1] International Telecommunication Union, Overview of the Internet of things, 2012.

[2] S. DuBravac, C. Ratti, The internet of things: Evolution or revolution?, 2015, (https://www.onr.com/blog/health-iot-adoption-hipaa-compliance-landscape/).

[3] Cloud Security Alliance, Security guidance for early adopters of the internet of things (iot), 2015.

[4] S. Ray, Y. Jin, A. Raychowdhury, The changing computing paradigm with internet of things: a tutorial introduction, IEEE Design Test 33 (2) (2016) 76–96.

[5] J. Guo, I. Chen, J.J.P. Tsai, A survey of trust computation models for service management in internet of things systems, Comput. Commun. 97 (2017) 1–14.

[6] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, J. Netw. Comput. Appl. 42 (2014) 120–134.

[7] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) (2013) 2266–2279.

[8] M. Wolf, D. Serpanos, Safety and security in cyber-physical systems and internet-of-things systems, Proc. IEEE 106 (1) (2018) 9–20.

[9] A. Banerjee, K.K. Venkatasubramanian, T. Mukherjee, S.K.S. Gupta, Ensuring safety, security, and sustainability of mission-critical cyberphysical systems, Proc. IEEE 100 (1) (2012) 283–299.

[10] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of things security: a survey, J. Netw. Comput. Appl. 88 (2017) 10–28.

[11] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: the road ahead, Comput. Netw. 76 (2015) 146–164.

[12] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: architecture, enabling technologies, security and privacy, and applications, IEEE Internet Things J. 4 (5) (2017) 1125–1142.

[13] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet of things: perspectives and challenges, Wireless Netw. 20 (8) (2014) 2481–2501.

[14] Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, A survey on security and privacy issues in internet-of-things, IEEE Internet Things J. 4 (5) (2017) 1250–1258.

[15] R. Minerva, A. Biru, D. Rotondi, Towards a definition of the internet of things (IoT), IEEE Internet Initative (2015) 1–86 Available on: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

[16] B.J. Mohd, T. Hayajneh, A.V. Vasilakos, A survey on lightweight block ciphers for low-resource devices: comparative study and open issues, J. Netw. Comput. Appl. 58 (2015) 73–93.

[17] S.R. Moosavi, T.N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, H. Tenhunen, SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways, Procedia Comput. Sci. 52 (2015) 452–459.

[18] W. Wu, L. Zhang, LBlock: a lightweight block cipher, in: International Conference on Applied Cryptography and Network Security, Springer, 2011, pp. 327–344.

[19] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, C. Vikkelsoe, PRESENT: an ultra-lightweight block cipher, in: Proceedings of the Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, pp. 450–466, doi:10.1007/978-3-540-74735-2_31.

[20] C.H. Lim, T. Korkishko, mCryptona lightweight block cipher for security of low-cost RFID tags and sensors, in: International Workshop on Information Security Applications, Springer, 2005, pp. 243–258.

[21] C. De Canniere, O. Dunkelman, M. Knežević, KATAN and KTANTANa family of small and efficient hardware-oriented block ciphers, in: Cryptographic Hardware and Embedded Systems-CHES 2009, Springer, 2009, pp. 272–288.

[22] A. Moradi, A. Poschmann, S. Ling, C. Paar, H. Wang, Pushing the limits: a very compact and a threshold implementation of AES, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2011, pp. 69–88.

[23] M.A. Orumiehchiha, J. Pieprzyk, R. Steinfeld, Cryptanalysis of WG-7: a lightweight stream cipher, Cryptography Commun. 4 (3–4) (2012) 277–285.

[24] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, C. Manifavas, A review of lightweight block ciphers, J. Cryptographic Engineering 8 (2) (2018) 141–184, doi:10.1007/s13389-017-0160-y.

[25] A.T. Lo'ai, T.F. Somani, More secure Internet of Things using robust encryption algorithms against side channel attacks, in: Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of, IEEE, 2016, pp. 1–6.

[26] F. Zhang, S. Guo, X. Zhao, T. Wang, J. Yang, F.X. Standaert, D. Gu, A framework for the analysis and evaluation of algebraic fault attacks on lightweight block ciphers, IEEE Trans. Inf. Forensics Secur. 11 (5) (2016) 1039–1054.

[27] M. Majzoobi, M. Rostami, F. Koushanfar, D.S. Wallach, S. Devadas, Slender PUF protocol: a lightweight, robust, and secure authentication by substring matching, Proceedings - IEEE CS Security and Privacy Workshops, SPW 2012 (2012) 33–44.

[28] C. Herder, M.-D. Yu, F. Koushanfar, S. Devadas, Physical unclonable functions and applications: a tutorial, Proc. IEEE 102 (8) (2014) 1126–1141.

[29] A. Seshadri, A. Perrig, L. Van Doom, P. Khosla, SWATT: software-based attestation for embedded devices, Proc. IEEE Symp. Secur. Privacy 2004 (2004) 272–282.

[30] A. Seshadri, M. Luk, E. Shi, A. Perrig, L. van Doorn, P. Khosla, Pioneer: verifying code integrity and enforcing untampered code execution on legacy systems, in: ACM SIGOPS Operating Systems Review, 39, ACM, 2005, pp. 1–16.

[31] A. Seshadri, M. Luk, A. Perrig, L. van Doorn, P. Khosla, Scuba: secure code update by attestation in sensor networks, in: Proceedings of the 5th ACM workshop on Wireless security, ACM, 2006, pp. 85–94.

[32] Y. Yang, X. Wang, S. Zhu, G. Cao, Distributed software-based attestation for node compromise detection in sensor networks, in: Reliable Distributed Systems, 2007. SRDS 2007. 26th IEEE International Symposium on, IEEE, 2007, pp. 219–230.

[33] T. AbuHmed, N. Nyamaa, D. Nyang, Software-based remote code attestation in wireless sensor network, in: Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, IEEE, 2009, pp. 1–8.

[34] K. Eldefrawy, G. Tsudik, A. Francillon, D. Perito, SMART: secure and minimal architecture for (Establishing Dynamic) root of trust., in: NDSS, 12, 2012, pp. 1–15.

[35] R. Strackx, F. Piessens, B. Preneel, Efficient isolation of trusted subsystems in embedded systems, in: International Conference on Security and Privacy in Communication Systems, Springer, 2010, pp. 344–361.

[36] J. Noorman, F. Freiling, J.V. Bulck, J.T. Mühlberg, F. Piessens, P. Maene, B. Preneel, I. Verbauwhede, J. Götzfried, T. Müller, Sancus 2.0: a low-cost security architecture for IoT devices, ACM Trans. Privacy Secur. 20 (3) (2017) 1–33.

[37] P. Koeberl, S. Schulz, A.-R. Sadeghi, V. Varadharajan, Trustlite: A security architecture for tiny embedded devices, in: Proceedings of the Ninth European Conference on Computer Systems, EuroSys '14, Amsterdam, The Netherlands, ACM, New York, NY, USA, 2014, pp. 10:1–10:14, doi:10.1145/2592798.2592824.

[38] F. Brasser, B. El Mahjoub, A.-R. Sadeghi, C. Wachsmann, P. Koeberl, TyTAN: tiny trust anchor for tiny devices, in: 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2015, IEEE, 2015, pp. 1–6.

[39] S. Schulz, A.-R. Sadeghi, C. Wachsmann, Short paper: Lightweight remote attestation using physical functions, in: Proceedings of the fourth ACM conference on Wireless network security, ACM, 2011, pp. 109–114.

[40] J. Kong, F. Koushanfar, P.K. Pendyala, A.-R. Sadeghi, C. Wachsmann, PUFatt: Embedded platform attestation based on novel processor-based PUFs, in: Proceedings of the 51st Annual Design Automation Conference, ACM, 2014, pp. 1–6.

[41] N. Asokan, F. Brasser, A. Ibrahim, A.-R. Sadeghi, M. Schunter, G. Tsudik, C. Wachsmann, SEDA: scalable embedded device attestation, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15 (2015) 964–975.

[42] M. Ambrosin, M. Conti, A. Ibrahim, G. Neven, A.-R. Sadeghi, M. Schunter, SANA: secure and scalable aggregate network attestation, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 731–742.

[43] T. Abera, N. Asokan, L. Davi, J.-E. Ekberg, T. Nyman, A. Paverd, A.-R. Sadeghi, G. Tsudik, C-FLAT: control-flow attestation for embedded systems software, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 743–754.

[44] G. Dessouky, S. Zeitouni, T. Nyman, A. Paverd, L. Davi, P. Koeberl, N. Asokan, A.-R. Sadeghi, LO-FAT: low-overhead control flow attestation in Hardware, in: Design Automation Conference (DAC), 2017 54th ACM/EDAC/IEEE, IEEE, 2017, pp. 1–6.

[45] T. Abera, N. Asokan, L. Davi, F. Koushanfar, A. Paverd, A.-R. Sadeghi, G. Tsudik, Things, trouble, trust: on building trust in IoT systems, in: Proceedings of the 53rd Annual Design Automation Conference, ACM, 2016, p. 121.

[46] T. Abera, N. Asokan, L. Davi, F. Koushanfar, A. Paverd, A.-R. Sadeghi, G. Tsudik, Invited - Things, trouble, trust, Proceedings of the 53rd Annual Design Automation Conference on - DAC '16 (3) (2016) 1–6.

[47] C. Kolias, G. Kambourakis, A. Stavrou, J.M. Voas, Ddos in the iot: mirai and other botnets, IEEE Comput. 50 (7) (2017) 80–84.

[48] M.D. Donno, N. Dragoni, A. Giaretta, A. Spognardi, Ddos-capable iot malwares: comparative analysis and mirai investigation, Secur. Commun. Netw. 2018 (2018) 7178164:1–7178164:30.

[49] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J.A. Halderman, L. Invernizzi, M. Kallitsis, Understanding the mirai botnet, in: USENIX Security Symposium, 2017, pp. 1092–1110.

[50] C. George, F. Glenn A., A. Mohammed, B. Jared, R. Nighot, M. Sukanya, A. Nagender, H. Chris, C. Lucian, INTERNET OF THINGS (IOT) SECURITY BEST PRACTICES, 2017.

[51] B. Lee, J. Lee, Blockchain-based secure firmware update for embedded devices in an internet of things environment, J. Supercomput. 73 (3) (2017) 1152–1167, doi:10.1007/s11227-016-1870-0.

[52] P. Ruckebusch, E. De Poorter, C. Fortuna, I. Moerman, Ad Hoc Networks 36 (2016) 127–151, doi:10.1016/j.adhoc.2015.05.017.

[53] J. Granjal, E. Monteiro, J.S. Silva, Security for the internet of things: a survey of existing protocols and open research issues, IEEE Commun. Surv. Tutorials 17 (3) (2015) 1294–1312.

[54] A. Burg, A. Chattopadhyay, K. Lam, Wireless communication and security issues for cyber-physical systems and the internet-of-things, Proc. IEEE 106 (1) (2018) 38–60.

[55] D. Airehrour, J.A. Gutiérrez, S.K. Ray, Secure routing for internet of things: a survey, J. Netw. Comput. Appl. 66 (2016) 198–213.

[56] M. Dohler, T. Watteyne, T. Winter, D. Barthel, Routing requirements for urban low-power and lossy networks, Technical Report, 2009.

[57] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.

[58] T. Winter, P. Thubert, A. Brandt, J.W. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, R.K. Alexander, RPL: Ipv6 routing protocol for low-power and lossy networks, RFC 6550 (2012) 1–157.

[59] Z. Shelby, C. Bormann, 6LoWpan: the wireless embedded internet, 43, John Wiley & Sons, 2011.

[60] P.L.R. Chze, K.S. Leong, A secure multi-hop routing for iot communication, in: IEEE World Forum on Internet of Things, WF-IoT 2014, Seoul, South Korea, March 6–8, 2014, IEEE Computer Society, 2014, pp. 428–432.

[61] C.H. Tseng, S.-H. Wang, C. Ko, K. Levitt, DEMEM: Distributed evidence–driven message exchange intrusion detection model for MANET, in: International Workshop on Recent Advances in Intrusion Detection, Springer, 2006, pp. 249–271.

[62] Y. Liu, M. Dong, K. Ota, A. Liu, Activetrust: secure and trustable routing in wireless sensor networks, IEEE Trans. Inf. Forensics Secur. 11 (9) (2016) 2013–2027.

[63] J. Duan, D. Yang, H. Zhu, S. Zhang, J. Zhao, TSRF: A trust-aware secure routing framework in wireless sensor networks, IJDSN 10 (2014), doi:10.1155/2014/209436.

[64] A. Ahmed, K.A. Bakar, M.I. Channa, K. Haseeb, A.W. Khan, A trust aware routing protocol for energy constrained wireless sensor network, Telecommun. Syst. 61 (1) (2016) 123–140.

[65] D. Airehrour, J.A. Gutiérrez, An analysis of secure MANET routing features to maintain confidentiality and integrity in iot routing, in: CONF-IRM 2015, The International Conference on Information Resources Management: Realizing the Digital Enterprise, Ottawa, Ontario, Canada, May 18–20, 2015, 2015, p. 17.

[66] D. Dragomir, L. Gheorghe, S. Costea, A. Radovici, A Survey on Secure Communication Protocols for IoT Systems, in: Secure Internet of Things (SIoT), 2016 International Workshop on, IEEE, 2016, pp. 47–62.

[67] H. Kim, E.A. Lee, Authentication and authorization for the internet of things, IT Prof. 19 (5) (2017) 27–33.

[68] A. Alcaide, E. Palomar, J. Montero-Castillo, A. Ribagorda, Anonymous authentication for privacy-preserving iot target-driven applications, Comput. Secur. 37 (2013) 111–123.

[69] C. Su, B. Santoso, Y. Li, R.H. Deng, X. Huang, Universally composable RFID mutual authentication, IEEE Trans. Dependable Secure Comput. 14 (1) (2017) 83–94.

[70] Y. Gao, G. Li, H. Ma, S.F. Al-Sarawi, O. Kavehei, D. Abbott, D.C. Ranasinghe, Obfuscated challenge-response: A secure lightweight authentication mechanism for PUF-based pervasive devices, in: Pervasive Computing and Communication Workshops (PerCom Workshops), 2016 IEEE International Conference on, IEEE, 2016, pp. 1–6.

[71] P. Cirne, A. Zúquete, S. Sargento, TROPHY: Trustworthy VANET routing with group authentication keys, Ad Hoc Netw. 71 (2018) 45–67.

[72] S.M. Pournaghi, B. Zahednejad, M. Bayat, Y. Farjami, NECPPA: a novel and efficient conditional privacy-preserving authentication scheme for VANET, Comput. Netw. 134 (2018) 78–92.

[73] K. Mahmood, S.A. Chaudhry, H. Naqvi, S. Kumari, X. Li, A.K. Sangaiah, An elliptic curve cryptography based lightweight authentication scheme for smart grid communication, Future Gener. Comput. Syst. 81 (2018) 557–565.

[74] L. Yan, Y. Chang, S. Zhang, A lightweight authentication and key agreement scheme for smart grid, IJDSN 13 (2) (2017) 1550147717694173, doi:10.1177/1550147717694173.

[75] A. Zhang, L. Wang, X. Ye, X. Lin, Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems, IEEE Trans. Inf. Forensics Secur. 12 (3) (2017) 662–675.

[76] S. Sutar, A. Raha, D.M. Kulkarni, R. Shorey, J.D. Tew, V. Raghunathan, D-PUF: an intrinsically reconfigurable DRAM PUF for device authentication and random number generation, ACM Trans. Embedded Comput. Syst. 17 (1) (2018) 17:1–17:31.

[77] L. Wu, J. Fan, Y. Xie, J. Wang, Q. Liu, Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks, IJDSN 13 (3) (2017).

[78] G. Peng, G. Zhou, D.T. Nguyen, X. Qi, Q. Yang, S. Wang, Continuous authentication with touch behavioral biometrics and voice on wearable glasses, IEEE Trans. Hum. Mach. Syst. 47 (3) (2017) 404–416.

[79] S. Ramachandran, V. Shanmugam, A two way authentication using bilinear mapping function for wireless sensor networks, Comput. Electr. Eng. 59 (2017) 242–249.

[80] T. Gao, X. Deng, N. Guo, X. Wang, An anonymous authentication scheme based on pmipv6 for vanets, IEEE Access 6 (2018) 14686–14698, doi:10.1109/ACCESS.2018.2810096.

[81] Q. Jiang, J. Ma, X. Lu, Y. Tian, An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks, Peer-to-peer Netw. Appl. 8 (6) (2015) 1070–1081.

[82] P. Gope, R. Amin, S.H. Islam, N. Kumar, V.K. Bhalla, Lightweight and privacy-preserving RFID authentication scheme for distributed iot infrastructure with secure localization services for smart city environment, Future Gener. Comp. Syst. 83 (2018) 629–637.

[83] C. Xu, M. Ma, X. Huang, H. Bao, A cross-domain group authentication scheme for LTE-A based vehicular network, in: Communication Software and Networks (ICCSN), 2017 IEEE 9th International Conference on, IEEE, 2017, pp. 595–599.

[84] B. Carminati, E. Ferrari, K.L. Tan, Enforcing access control over data streams, in: Proceedings of the 12th ACM symposium on Access control models and technologies, ACM, 2007, pp. 21–30.

[85] E. Barka, S.S. Mathew, Y. Atif, Securing the web of things with role-based access control, in: International Conference on Codes, Cryptology, and Information Security, Springer, 2015, pp. 14–26.

[86] N. Ye, Y. Zhu, R.C. Wang, R. Malekian, Q.M. Lin, An efficient authentication and access control scheme for perception layer of internet of things, Appl. Math. Inf. Sci. 8 (4) (2014) 1617–1624.

[87] G. Zhang, W. Gong, The research of access control based on UCON in the internet of things, JSW 6 (4) (2011) 724–731.

[88] P.N. Mahalle, B. Anggorojati, N.R. Prasad, R. Prasad, Identity authentication and capability based access control (iacac) for the internet of things, J. Cyber Secur. Mobility 1 (4) (2013) 309–348.

[89] M. Shahzad, M.P. Singh, Continuous authentication and authorization for the internet of things, IEEE Internet Comput. 21 (2) (2017) 86–90.

[90] R. Neisse, G. Steri, I.N. Fovino, G. Baldini, Seckit: a model-based security toolkit for the internet of things, Comput. Secur. 54 (2015) 60–76.

[91] J.E. Kim, G. Boulos, J. Yackovich, T. Barth, C. Beckel, D. Mosse, Seamless integration of heterogeneous devices and access control in smart homes, in: Intelligent Environments (IE), 2012 8th International Conference on, IEEE, 2012, pp. 206–213.

[92] N. Saxena, B.J. Choi, R. Lu, Authentication and authorization scheme for various user roles and devices in smart grid, IEEE Trans. Inf. Forensics Secur. 11 (5) (2016) 907–921.

[93] Q. Tasali, C. Chowdhury, E.Y. Vasserman, A flexible authorization architecture for systems of interoperable medical devices, in: Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, ACM, 2017, pp. 9–20.

[94] R.H. Weber, Internet of things: privacy issues revisited, Comput. Law Secur. Rev. 31 (5) (2015) 618–627.

[95] J.H. Ziegeldorf, O.G. Morchon, K. Wehrle, Privacy in the internet of things: threats and challenges, Secur. Commun. Netw. 7 (12) (2014) 2728–2742.

[96] J. López, R. Rios, F. Bao, G. Wang, Evolving privacy: from sensors to the internet of things, Future Gener. Comp. Syst. 75 (2017) 46–57.

[97] R. Mendes, J.P. Vilela, Privacy-preserving data mining: methods, metrics, and applications, IEEE Access 5 (2017) 10562–10582.

[98] M. Al-Rubaie, J.M. Chang, Privacy preserving machine learning: Threats and solutions, CoRR (2018). arXiv: 1804.11238.

[99] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, N. Feamster, Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic, CoRR (2017). arXiv: 1708.05044.

[100] J. Liu, C. Zhang, Y. Fang, EPIC: a differential privacy framework to defend smart homes against internet traffic analysis, IEEE Internet Things J. 5 (2) (2018) 1206–1217.

[101] T. Song, R. Li, B. Mei, J. Yu, X. Xing, X. Cheng, A privacy preserving communication protocol for IoT applications in smart homes, in: Identification, Information and Knowledge in the Internet of Things (IIKI), 2016 International Conference on, IEEE, 2016, pp. 519–524.

[102] B. Riedl, V. Grascher, T. Neubauer, A secure e-health architecture based on the appliance of pseudonymization, JSW 3 (2) (2008) 23–32.

[103] J. Heurix, S. Fenz, A. Rella, T. Neubauer, Recognition and pseudonymisation of medical records for secondary use, Med. Biol. Eng. Comput. 54 (2–3) (2016) 371–383.

[104] X. Liu, Y. Li, J. Qu, Y. Ding, A lightweight pseudonym authentication and key agreement protocol for multi-medical server architecture in TMIS, TIIS 11 (2) (2017) 924–944.

[105] X. Li, M.H. Ibrahim, S. Kumari, A.K. Sangaiah, V. Gupta, K.-K.R. Choo, Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks, Comput. Netw. 129 (2017) 429–443.

[106] S. Wang, N. Yao, LIAP: A local identity-based anonymous message authentication protocol in VANETs, Comput. Commun. 112 (2017) 154–164.

[107] A.M. Koya, P.P. Deepthi, Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network, Comput. Netw. 140 (2018) 138–151.

[108] K. Seol, Y.-G. Kim, E. Lee, Y.-D. Seo, D.-K. Baik, Privacy-preserving attribute-based access control model for XML-based electronic health record system, IEEE Access 6 (2018) 9114–9128.

[109] C.-I. Fan, S.-Y. Huang, Y.-L. Lai, Privacy-enhanced data aggregation scheme against internal attackers in smart grid, IEEE Trans. Ind. Inf. 10 (1) (2014) 666–675.

[110] H. Shen, M. Zhang, J. Shen, Efficient privacy-preserving cube-data aggregation scheme for smart grids, IEEE Trans. Inf. Forensics Secur. 12 (6) (2017) 1369–1381.

[111] M.A. Rahman, M.H. Manshaei, E. Al-Shaer, M. Shehab, Secure and private data aggregation for energy consumption scheduling in smart grids, IEEE Trans Dependable Secure Comput. 14 (2) (2017) 221–234.

[112] G. Giaconi, D. Gündüz, H.V. Poor, Privacy-aware smart metering: progress and challenges, IEEE Signal Process. Mag. 35 (6) (2018) 59–78, doi:10.1109/MSP.2018.2841410.

[113] G. Giaconi, D. Gündüz, H.V. Poor, Smart meter privacy with renewable energy and an energy storage device, IEEE Trans. Inf. Forensics Secur. 13 (1) (2018) 129–142.

[114] Y. Tian, N. Zhang, Y. Lin, X. Wang, B. Ur, X. Guo, P. Tague, Smartauth: User–centered authorization for the internet of things, in: E. Kirda, T. Ristenpart (Eds.), 26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16–18, 2017., USENIX Association, 2017, pp. 361–378.

[115] E. Fernandes, A. Rahmati, J. Jung, A. Prakash, Security implications of permission models in smart-home application frameworks, IEEE Secur. Privacy 15 (2) (2017) 24–30.

[116] M.A. Sahi, H. Abbas, K. Saleem, X. Yang, A. Derhab, M.A. Orgun, W. Iqbal, I. Rashid, A. Yaseen, Privacy preservation in e-Healthcare environments: state of the art and future directions, IEEE Access 6 (2018) 464–478.

[117] C. Rottondi, G. Verticale, A. Capone, Privacy-preserving smart metering with multiple data consumers, Comput. Netw. 57 (7) (2013) 1699–1713.

[118] S. Ge, P. Zeng, R. Lu, K.R. Choo, FGDA: fine-grained data analysis in privacy-preserving smart grid communications, Peer-to-Peer Networking and Applications 11 (5) (2018) 966–978, doi:10.1007/s12083-017-0618-9.

[119] D. Engel, G. Eibl, Wavelet-based multiresolution smart meter privacy, IEEE Trans. Smart Grid 8 (4) (2017) 1710–1721.

[120] S. Zawoad, R. Hasan, Faiot: Towards building a forensics aware eco system for the internet of things, in: 2015 IEEE International Conference on Services Computing (SCC), IEEE, 2015, pp. 279–284.

[121] L. Caviglione, S. Wendzel, W. Mazurczyk, The future of digital forensics: challenges and the road ahead, IEEE Secur. Privacy (6) (2017) 12–17.

[122] M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of things security and forensics: challenges and opportunities, Future Gener. Comput. Syst. 78 (2018) 544–546.

[123] V.R. Kebande, I. Ray, A generic digital forensic investigation framework for internet of things (iot), in: Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on, IEEE, 2016, pp. 356–362.

[124] E. Oriwoh, D. Jazani, G. Epiphaniou, P. Sant, Internet of things forensics: challenges and approaches, in: Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on, IEEE, 2013, pp. 608–615.

[125] A. Nieto, R. Rios, J. Lopez, IoT-Forensics meets privacy: towards cooperative digital investigations, Sensors 18 (2) (2018) 492.

[126] Changing driving laws to support automated vehicles, (http://www.ntc.gov.au/current-projects/changing-driving-laws-to-support-automated-vehicles/?modeId=1064&topicId=1166).

[127] I.G. Harris, Social Engineering Attacks on the Internet of Things, (https://iot.ieee.org/newsletter/september-2016/social%2Dengineering%2Dattacks%2Don%2Dthe%2Dinternet%2Dof%2Dthings.html).

[128] GDPR Portal: Site Overview, (https://www.eugdpr.org/).

[129] Y. O'Connor, W. Rowan, L. Lynch, C. Heavin, Privacy by design: informed consent and internet of things for smart health, Procedia Comput. Sci. 113 (2017) 653–658.

[130] Health Insurance Portability and Accountability Act, (https://en.wikipedia.org/wiki/Health%7B_%7DInsurance%7B_%7DPortability%7B_%7Dand%7B_%7DAccountability%7B_%7DAct).

Jianwei Hou received the B.S. degree in information security from Harbin Engineering University, Harbin, P.R. China, in 2016. She is currently pursuing the Ph.D. degree at the School of Information, Renmin University of China, Beijing, P.R. China. Her research interests include system security, software-defined networking, and IoT security.

Leilei Qu received the B.S. degree in information security from Renmin University of China, Beijing, P.R. China, in 2017. She is currently working towards the Ph.D. degree at the School of Information, Renmin University of China. Her research interests include system security, IoT security and human factors in cybersecurity.

Wenchang Shi received his B.S. degree in computer science from the Department of Computer Science and Technology, Peking University, Beijing, P.R. China, and his Ph.D. degree in computer science from the Institute of Software, Chinese Academy of Sciences, Beijing, P.R.China. Currently, he is a Professor at School of Information, Renmin University of China, Beijing, P.R. China. He is a member of the Steering Committee of Cybersecurity Education, Ministry of Education, China, the vice president of the China Cyber and Information Law Society, and the Vice Chair of the Academic Committee, China Cloud Security Alliance. His research interests include System Security, Trusted Computing and Digital Forensics.