A Survey on Digital Forensics in Internet of Things

Jianwei Hou, Yuewei Li, Jingyang Yu, and Wenchang Shi

***Abstract*—Internet of Things (IoT) is increasingly permeating peoples' lives, gradually revolutionizing our way of life. Due to the tight connection between people and IoT, now civil and criminal investigations or internal probes must take IoT into account. From the forensic perspective, the IoT environment contains a rich set of artifacts that could benefit investigations, while the forensic investigation in IoT paradigm may have to alter to accommodate characteristics of IoT. Therefore, in this article, we analyze the impact of IoT on digital forensics and systematize the research efforts made by previous researchers from 2010 to 2018. We sketch the landscape of IoT forensics and examine the state of IoT forensics under a 3-D framework. The 3-D framework consists of a temporal dimension, a spatial dimension, and a technical dimension. The temporal dimension walks through the standard digital forensic process while the spatial dimension explores where to identify sources of evidence in IoT environment. These two dimensions attempt to provide principles and guidelines for standardizing digital investigations in the context of IoT. The technical dimension guides a way to the exploration of tools and techniques to ensure the enforcement of digital forensics in the ever-evolving IoT environment. Put together, we present a holistic overview of digital forensics in IoT. We also highlight open issues and outline promising suggestions to inspire future study.**

***Index Terms*—Cybercrime, digital forensics, Internet of Things (IoT).**

I. Introduction

With the Internet of Things (IoT) permeating our daily lives, people are becoming more reliant on various kinds of smart IoT services, leaving traces on various IoT devices. These rich repositories of digital traces in IoT environment can provide insight into people's daily activities in their home and elsewhere, which are of great value to digital forensics [1]. On the other hand, the number of both civil and criminal cases involving IoT devices or services has grown. IoT devices may not only be targets for attacks, but also tools for committing crimes. Security vulnerabilities in IoT systems can be leveraged to remotely control the systems, for example, to control the accelerator and brake system of the smart vehicle to cause an incident. Therefore, there is an urgent need for IoT forensics research to assist in determining the who, what, where, when, and how for cases.

The rapid adoption of IoT expands the range of digital evidence from the PC or laptops to a wide range of IoT devices (e.g., wearable devices and automobiles) as well as various cloud-based IoT services, which presents multifaceted challenges for investigators. Although current forensic methodologies and tools still prove useful at some stages of forensics in IoT domain, there is still a pressing need to update current tools, procedures, and legislation to deal with unique characteristics of IoT [2].

The main goal of this survey is to have an overview of the state of IoT forensics and provide guidelines for future research and practices on it. We try to provide a comprehensive and structured landscape of IoT forensics under a 3-D framework. The framework encompasses a temporal dimension, a spatial dimension, and a technical dimension.

From the temporal dimension, IoT forensics follows the standard digital forensic process including collection, examination, analysis, and reporting to transform media into evidence and calls for appropriate forensic models to support the reasonable and appropriate use of forensic tools for practical investigations involving IoT. From the spatial dimension, we explore IoT forensics with respect to the forensic environment where potential evidence may exist. Based on the typical architecture of IoT, the major sources of evidence in IoT forensics can be divided into three domains, i.e., device, network, and cloud. From the technical dimension, we investigate IoT forensics by exploring the enabling methods, tools, or techniques that can provide the ability to collect and examine volatile or nonvolatile data and to perform quick reviews or in-depth analysis of data from various sources of evidence in IoT environment.

Together with the three dimensions, we make a systematic analysis of existing efforts on digital forensics in IoT paradigm to present a holistic overview of this domain. We also point out open issues that IoT forensics faces and put forward promising suggestions to assist with future research. The main contributions of this article are highlighted as follows.

1) We discuss and summarize the impact of IoT on digital forensics according to fundamental characteristics of IoT.
2) We provide an overview of existing research efforts from 2010 to 2018 on IoT forensics and briefly introduce the development of IoT forensics.
3) We sketch the landscape of IoT forensics and review the state of it under a 3-D framework.
4) We highlight the open issues in the field of IoT forensics and propose corresponding suggestions.

Manuscript received May 9, 2019; revised July 9, 2019; accepted August 26, 2019. Date of publication September 11, 2019; date of current version January 10, 2020. This work was supported in part by the National Natural Science Foundation of China under Grant 61472429, in part by the Natural Science Foundation of Beijing Municipality under Grant 4122041, and in part by the National High Technology Research and Development Program of China under Grant 2007AA01Z414. *(Corresponding author: Wenchang Shi.)*

J. Hou, Y. Li, and W. Shi are with the School of Information, Renmin University of China, Beijing 100872, China (e-mail: houjianwei@ruc.edu.cn; well_li@ruc.edu.cn; wenchang@ruc.edu.cn).

J. Yu is with the School of Information, Renmin University of China, Beijing 100872, China, and also with the School of Computer and Information Engineering, Henan University, Kaifeng 475004, China (e-mail: yjy@henu.edu.cn).

Digital Object Identifier 10.1109/JIOT.2019.2940713

The remainder of this article is organized as follows. In Section II, we introduce the background of digital forensics and discuss the impact of IoT on digital forensics. We also introduce smart home as a typical IoT scene that helps to illustrate digital forensics in IoT environment later in the following sections. In Section III, we select and investigate the recent literature on IoT forensics and clarify the development of IoT forensics research. We sketch the landscape of IoT forensics under a 3-D framework in Section IV and illustrate each dimension in detail in Sections V–VII, respectively. In Section VIII, from the three dimensions, we highlight the open issues and present promising suggestions for future research and practices in the field of IoT forensics. Finally, we conclude this article in Section IX.

II. Background

A. Digital Forensics

Digital forensics aims to gain a better understanding of an event of interest by finding and analyzing the facts related to that event [3]. The digital forensic investigators reveal the truth of an event by discovering and exposing the remnants (footprints or artifacts) of an event left on the digital system.

The NIST Recommendation [4] has divided the digital forensic investigation process into four consecutive (or iterative if necessary) phases, i.e., collection, examination, analysis, and reporting. Although different sources of evidence may call for different methodologies and generate different types of evidence, digital investigations in IoT environment still need to be carried out under this process to support the admissibility of evidence in legal processing.

B. Forensic Soundness

Forensic soundness is the basic principle for forensic investigations. On the one hand, it refers to the fact that the digital forensic process must follow a certain standard so that it can be admissible in a court of law. On the other hand, the application or development of forensic tools and techniques should be undertaken in accordance with the relevant rules of forensics to protect the evidence from damage. A process is considered to be forensically sound if it meets the following four criteria [5].

1) *Meaning:* The forensic process cannot change the original meaning of evidence or should try to have the minimum change.
2) *Errors:* The forensic process should avoid undetectable errors and any error in the process should be properly documented.
3) *Transparency and Trustworthiness:* The reliability and accuracy of the forensic process are capable of being tested and/or verified by, for example, an external examination of the forensic procedures by a court of law.
4) *Experience:* The individuals undertaking the forensic investigation should have sufficient experience or knowledge and should not undertake an examination that is beyond his/her current level of knowledge and skill.

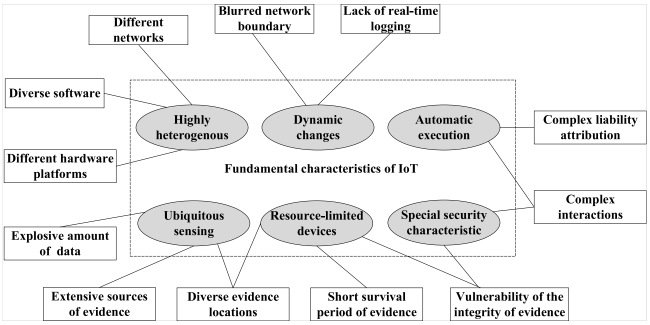
Different networks
Blurred network boundary
Lack of real-time logging
Diverse software
Highly heterogenous
Dynamic changes
Automatic execution
Complex liability attribution
Different hardware platforms
Fundamental characteristics of IoT
Explosive amount of data
Ubiquitous sensing
Resource-limited devices
Special security characteristic
Complex interactions
Extensive sources of evidence
Diverse evidence locations
Short survival period of evidence
Vulnerability of the integrity of evidence

Fig. 1. Impact of IoT on digital forensics.

C. Impact of IoT on Digital Forensics

IoT enables more and more devices "online," providing various kinds of smart services (e.g., smart city, medical care, and smart home) that are bound up with peoples' lives. Considering the fundamental characteristics of IoT, we discuss the impact of IoT on digital forensics, summarized in Fig. 1.

1) Ubiquitous Sensing: With temperature sensors, motion detectors, or pressure sensors, IoT devices have the ubiquitous sensing ability so that they contain potential evidence closely related to the behavior of their owners and other devices in their environments [6]. More diverse sources of evidence and fine-grained sensing in IoT contribute to reconstructing the context of cases, which also produces a large volume of forensic data needing to be dealt with.

2) Dynamic Changes: The state of IoT devices changes dynamically. That is, a device may join or leave a network autonomously or with the movement of users at any time. Due to such temporal and spatial change properties, network topologies change dynamically and network boundaries become blurry, which would make it more difficult to identify the boundaries of cases [7]. The dynamic feature of IoT calls for real-time logging to record temporal information, such as modified time, accessed time, and created time, which can help to correlate and sequence the digital evidence gathered from different devices.

3) Automated Execution: There are real-time and automated interactions between IoT devices to facilitate the collaboration between different IoT applications [8]. Devices may operate automatically according to the information from surroundings or other entities, reducing human intervention. Within automated systems, there are questions of control (who/what did it?) and responsibility (who/what is at fault?) while the increase of interactions makes it prohibitively complex to trace back incidents through a chain of different devices.

4) Resource-Limited Characteristic of Devices: Due to the limited resources of some IoT devices, data on the devices may have a short survival period before being overwritten by the latest data and is usually sent to cloud or other data center. Therefore, it is more difficult to locate where potential evidence may exist. On the other hand, these resource-limited devices may be in the absence of adequate security guarantee, so that malicious users may easily modify or destroy the logs and relevant data on the devices [9].

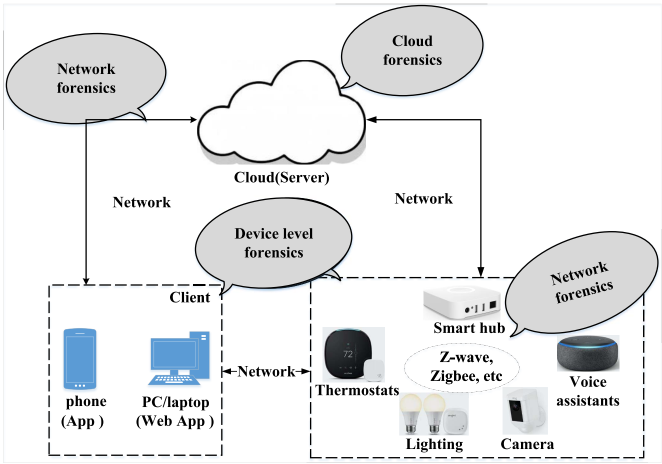

Fig. 2. IoT forensics paradigm of smart home.

5) Highly Heterogeneous: Based on different hardware, software, and networks, IoT devices are heterogeneous with multiple protocols, diverse data formats, and proprietary interfaces. Types of data in IoT forensics may be diverse in various vendor-specific formats. Heterogeneous devices may call for different tools or methods for data collection, examination, and analysis, which requires more efforts for investigators. The contemporary forensic tools may not be able to deal with every source of evidence, which calls for new tools. New tools should be properly tested and assessed prior to their use [5] because unreliable tools may lead to uncertainty and loss, and affect the soundness of evidence and even the final conclusion.

6) Special Security Characteristic: IoT bridges the gap between the cyber world and the physical world, so that security threats in the cyber world can bring safety threats to the real-world and vice versa [10]. IoT enables the communication abilities to various kinds of devices (e.g., smart appliances, connected vehicles, and personal health devices) and connects them to the network, which may lead to broad attack faces. A single IoT device can be used to compromise other connected devices due to the connection between devices, which will transfer or expand the impact and increase the complexity of forensics. Moreover, due to the integration of the cyber world and the physical world, IoT devices can be remotely controlled to operate the physical world. Therefore, unsafe and insecure operations on IoT devices may result in a real loss of services and even the loss of life. There is a growing need for forensics to reconstruct security/safety incidents or troubleshoot the operational problems in IoT systems. And the security threat that adversaries can remotely control the device to remove or modify traces (e.g., logs and videos) or even destroy the device may make the evidence fragile and compromise the integrity of evidence.

D. *Typical IoT Scene*

Smart home is a typical application scenario in IoT including three layers of a typical IoT architecture: 1) a sensing layer; 2) a networking and data communication layer; and 3) an application layer.

A smart home system is usually composed of a hub, multiple IoT devices, and a back-end server (e.g., a cloud), as shown in Fig. 2. Thermostats, lightings, cameras, and voice assistants are endpoint IoT devices in the sensing layer to measure, collect, and process the state information associated with these things. These devices use wired or wireless communication protocols to communicate in the network and data communication layer. They can communicate through the Internet via the hub or directly through a local network. The hub can send the data from devices to the back-end cloud for storage, processing, and application. Users can control the devices or obtain status information of devices by sending commands to the cloud through Apps on mobile phones or Webs. Then the hub receives commands from the server and sends them to the devices, so that devices will execute relevant operations according to the commands. Devices may also collaborate with each other automatically according to predefined conditions.

We will take this typical IoT scene as an example to illustrate in detail the digital forensics in the IoT environment from different perspectives later.

III. Literature Review on IoT Forensics

A. *Literature Selection Process*

In order to have a clear picture of digital forensics in the IoT environment, this section provides an extensive literature review of the research on IoT forensics. This article selection strategy consists of three main stages.

1) *Stage 1:* Define the keywords to search relevant papers from electronic databases (DBLP, IEEE Xplorer, and Science Direct). Considering the alternatives and other synonyms of essential components of the keywords, the subsequent exploration string was defined: *("Forensic" OR "Investigation" OR "Evidence") AND ("Things" OR "Internet of Things" OR "IoT" OR "Smart").*
2) *Stage 2:* Select papers based on the title, publication year, and language of them (only includes the papers written in English). To ensure that only high-quality publications were included in the study, we focus on journal publications and conferences papers published by Elsevier, IEEE, Springer, ACM, and Wiley. Moreover, opinion-driven reports (editorials, commentaries, and letters) and books were excluded.
3) *Stage 3:* Review the abstracts and full texts of the selected papers to verify the relevance of these papers. The cited information, abstracts, and keywords of the papers were recorded for further analysis.

Finally, 58 papers published between 2010 and 2018 were extracted through the three phases, as shown in Table I.

B. *Overview of Existing Research on IoT Forensics*

From the distribution of the papers by the year of publication from 2010 to 2018, there is a sharp increase number of papers in 2018 and all the other years witness a gradual increase. Research on IoT forensics has entered a new

TABLE I
DISTRIBUTION OF EXISTING RESEARCH ON IOT FORENSICS

Year	Publisher	Survey	Forensic System	Forensic Model	Forensic Method	Tools and Techniques
2010	Elsevier					
	IEEE					
	Springer				[11]	
	ACM					
	Weiley					
2012	Elsevier					
	IEEE					[12]
	Springer					
	ACM					
	Weiley					
2013	Elsevier					
	IEEE		[13], [14]	[2]		
	Springer					
	ACM					
	Weiley					
2014	Elsevier	[15]			[16]	[17]–[19]
	IEEE					
	Springer					
	ACM					
	Weiley					
2015	Elsevier					[20]
	IEEE		[21]	[22]		
	Springer					
	ACM				[23]	
	Weiley					
2016	Elsevier	[9]				[24]
	IEEE		[25]	[26], [27]	[28]	[6]
	Springer					
	ACM	[29]				
	Weiley					
2017	Elsevier	[30]	[31], [32]		[33]	
	IEEE		[34]–[36]	[37]		[38]
	Springer		[39]			[40]
	ACM			[1], [41]		
	Weiley					
2018	Elsevier	[42]			[43], [44]	[45]
	IEEE	[46]–[48]	[49]–[52]	[53]		[54], [55]
	Springer	[56], [57]			[58], [59]	[60], [61]
	ACM				[62]	[63]
	Weiley	[64]				

period of significant growth since 2016 with the wide application of IoT devices in production and life. The 58 papers are classified under five categories including survey papers, models/frameworks, forensic methods, forensic systems, and forensic techniques/tools.

From 2010 to 2018, there was ongoing research on forensic methods to provide guidelines for investigations on different sources of evidence in IoT and explore feasible forensic methods and techniques. The greater part of the work studies enabling forensic techniques and tools for the coming new demands and challenges of digital forensics in IoT environment, concerning evidence collection, examination, and analysis.

Early work on IoT forensics was predominantly theoretical in nature, and aimed to deal with issues about frameworks and models. In 2013, Oriwoh *et al.* [2] first explored the conceptual digital forensic models for IoT forensics to guide forensic investigations involving the IoT, which provided the basis for further research on forensic models and frameworks. At the same time, they also explored the automated forensic system that aims to make the IoT environment forensically ready before potential cases occur [14]. The two research efforts laid the foundation of research on IoT forensics. Since then, there have been a great number of papers exploring IoT forensic frameworks/models to guide procedures for routine forensic tasks and developing forensic systems to ensure forensic readiness abilities for IoT.

Some survey papers [9], [46]–[48], [56], [57], [64] have made a preliminary exploration of challenges in IoT forensics. Chernyshev *et al.* [46] mainly focused on conceptual digital forensic models that can be applied to IoT environment. Bréda *et al.* [48] analyzed the minimal functional forensic requirements of IoT devices to provide reliable information. The requirements are defined in the user data protection class by the access control policy, the access control functions, the data authentication, and integrity requirements of the stored data to maintain a minimum level of data integrity in the IoT environment. Losavio *et al.* [64] analyzed in detail the legal concerns on data collection and analysis in IoT forensics.

There are also some surveys investigating IoT forensics in different IoT applications. The works in [15], [29], [30], [42] focus on forensic challenges associated with smart TVs, health and fitness related devices, vehicles, and smart cities, respectively.

In this article, we aim to outline the landscape of digital forensics in the IoT paradigm to provide guidance for forensic practitioners and researchers. We conduct a systematic review of the research status of IoT forensics under a 3-D framework and indicate future research directions.

IV. Landscape of IoT Forensics

IoT forensics is a branch of digital forensics that carries out digital forensics in the IoT environment. Forensic researchers and practitioners have tried to make digital forensics applicable to the context of IoT. Therefore, IoT forensics still follows the principles of digital forensics. It consists of two basic aspects. One is the forensic investigation itself and the other is the ability that enables the forensic investigation.

Within a forensic investigation process, data is extracted from various media, then is transformed into information, and finally becomes evidence that can be legally acceptable in a court of law [4]. Therefore, from the perspective of forensic investigations, there are two core questions, including how to obtain evidence and where to find evidence. The temporal dimension explores how to generate legally accepted and reliable evidence in line with a standard forensic process in IoT environment, including collection, examination, analysis, and reporting. The spatial dimension focuses on completely identifying potential sources of evidence, that is, to answer where to find evidence. Case-related information in IoT can be collected from different data sources that can be grouped into three types, i.e., device, network, and cloud, based on the typical IoT architecture.

On the other hand, technical abilities to enable forensic investigations also play important roles in the landscape of IoT forensics. The technical dimension aims to explore appropriate techniques/tools for data collection, examination, and analysis. As the forensic environment changes, IoT poses challenges to existing forensic techniques/tools that need to update to deal with the forensics task in IoT environment. Based on our survey, contemporary research on technical preparations for IoT forensics can be broadly divided into three categories including forensic readiness techniques, evidence extraction tools or techniques for different data sources, and some other forensic techniques to resolve challenges in IoT forensics.

Moreover, IoT forensics is under the legal principle. All activities and actions within investigations start with authorization and must comply with laws and regulations in the jurisdictions.

We then survey the literature on forensics in IoT environment under a unified framework consisting of three orthogonal coordinates, as shown in Fig. 3. We try to illustrate in detail various aspects of IoT forensics, which may help forensic researchers and practitioners with a systematic understanding of this domain.

V. IoT Forensics From the Temporal Dimension

From the temporal dimension, a forensic investigation in IoT environment should be conducted within the standard process, so that the collected evidence can be admissible on the court.

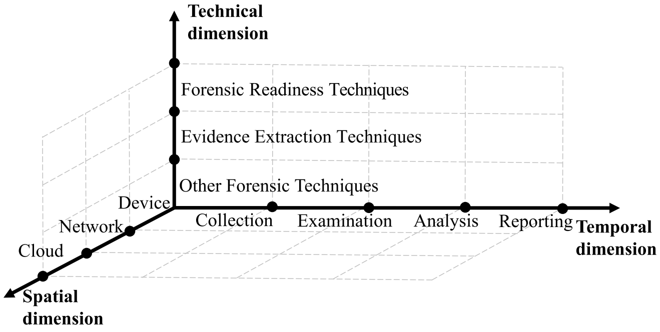

Fig. 3. Landscape of IoT forensics with three dimensions.

A. Forensic Process in Smart Home Scene

When performing a forensic investigation in a smart home scene described in Section II, investigators need to identify objects of forensic interest (OOFIs) on the spot first, including smart camera, voice assistants and some other appliances. These smart appliances on the spot connect to network devices (i.e., smart hub) to communicate with the external environment. So network traffic, cloud, and companion Apps on cell phones or PCs also need to be included in the investigation. First responders should consider the possible need to collect volatile data, which can be collected only from a live system that has not been rebooted or shut down since the event occurred.

Then, investigators need to examine the data obtained from OOFIs using specialized forensic toolkits to screen out the data related to the case. Therefore, investigators need to parse the data of different formats, which not only includes the data with relatively uniform formats from the phones and PCs but also the data with proprietary formats from various IoT devices.

Next, investigators correlate the data from different sources to identify people, places, items, events, and their relations to construct the facts of the case. For example, thermostat readings and lighting records may prove the presence of users when someone claimed he was out of the home and videos from cameras may show the individuals' behaviors at home.

The three phases above can be iterative because new sources of evidence could be revealed during the analysis of data.

Finally, investigators need to review the actions performed in the above three phases to ensure that all evidence reaches a definitive explanation of what happened. They also need to report in detail the results of the analysis, which may include describing the actions already performed, explaining how tools and procedures were selected, and determining what other actions need to be performed.

B. Research on Forensic Models for IoT Forensics

As a branch of digital forensics, there is a consensus that IoT forensics follows the four-phase forensic process. However, there is no accepted digital forensic model that can help to conduct digital investigations in an IoT-based environment. Some research aims to explore general and standard forensic models to facilitate consistent, effective, and accurate actions in forensic investigations involving IoT.

Oriwoh *et al.* [2] proposed a 1-2-3 zone approach and a nest-best-thing (NBT) approach for evidence acquisition within the IoT domain. The 1-2-3 zone approach divided the investigation area into three zones: 1) the internal network; 2) the middle; and 3) the external network. The evidence extraction process in each zone can be conducted in parallel. The NBT triage model assists with the identification of additional sources of evidence when the primary source is unavailable. The two models are of guiding significance in the identification stage in IoT-based investigations.

Perumal *et al.* [22] have proposed a top-down model that follows the standard operating procedures (SoPs). During the investigation, this model starts with authorization and planning. It introduces machine to machine (M2M) communication and integrates 1-2-3 zone model and triage model with the general forensic process to deal with IoT-based investigations. Although this paper gives a complete model covering each stage of the digital forensic process, it mainly focuses on identification without dealing with analysis and other processes.

Rahman *et al.* [26] have highlighted the importance of forensic readiness and proposed a forensic-by-design framework for cyber-physical cloud systems (CPCSs) based on ISO/IEC 27043:2015 [66]. The framework has defined the design principles of CPCS to facilitate forensic investigations. The principles comprise six factors, including risk management principles and practices, forensic readiness principles and practices, incident-handling principles and practices, laws and regulations, CPCS hardware and software requirements, and industry-specific requirements.

DFIF-IoT [27] is a complete forensic framework to guide digital investigations in IoT-based infrastructures. The framework is composed of proactive process, IoT forensics, reactive process, and concurrent process. Proactive process aims to make IoT environment forensically ready. IoT forensics consists of cloud forensics, network forensics, and device level forensics. Reactive process is consistent with the traditional forensic investigation process and will be performed in response to an incident of forensic concerns. Concurrent process is conducted throughout the whole process involving obtaining authorization, documentation, preservation of the chain of custody, physical investigation, and interaction with physical investigations. Under the consideration of a complex set of relationships among different IoT entities, IDFIF-IoT [65] extended DFIF-IoT framework. Discussion of interactions in IoT ecosystems can assist with the planning process for gathering, storing, and handling digital evidence in advance before investigation. The two frameworks cover the complete forensic process, and are insightful in standardization of IoT-based forensic process. However, the recognition of the frameworks still needs to be discussed further by all stakeholders.

FSAIoT [41] pointed out that states of IoT devices or the changes of states could be of forensic value. It proposed a model for the state acquisition of plenty of IoT devices to deal with forensics on IoT devices. This paper implemented the prototype of the framework, which can acquire states of devices from devices, clouds, and controllers, to prove its availability.

Zia *et al.* [1] proposed an application-specific digital forensic model for IoT forensics. The model provides guidelines for forensic investigations in different IoT application scenarios. To explain the model, the paper took three IoT application scenarios as examples, including smart city, smart home, and wearable devices, and pointed out a variety of evidence of forensic interests in the three scenarios.

Combining the NBT approach and 1-2-3 zone approach, Harbawi and Varol [37] proposed a last-on-scene (LoS) algorithm for effective evidence acquisition in IoT-based investigations. It assume that the last device in the communication chain should be investigated first. During the investigation, the LoS algorithm should be applied to each zone to identify sources of evidence in order, starting from the first zone. The LoS algorithm can simplify the process of evidence acquisition, but some real-time data in zones 2 and 3 may not be properly handled in time.

A summary of forensic models in the IoT paradigm is shown in Table II. These efforts are in the early stage, developing theoretical process models based on hypothetical case studies. They still require extensive scientific validation in practice. Although the actual investigation procedures may have to alter to adapt to every situation, forensic practitioners and researchers need to standardize the models for performing routine tasks on the logical level, which need to be approved by all stakeholders of IoT forensics.

VI. IoT Forensics From the Spatial Dimension

IoT is bringing more and more devices online, generating an explosion of connected devices, from refrigerators, cars, and drones, to smart grids and intelligent buildings [47]. OOFIs may be dispersed throughout IoT environment. OOFIs are no longer restricted to computers or servers, but can be found in vehicles, RFID cards, and refrigerators, which might be excluded in traditional forensic investigations. In this section, from the spatial dimension, we explore the forensic environment for IoT forensics under the architecture of IoT, concerning where the evidence may exist.

A. Sources of Evidence in IoT Environment

We first take the smart home scene to illustrate where to find potential sources of evidence in IoT-based investigations.

A person's physical actions continuously generate multiple telemetry streams across a myriad of wireless devices, cloud environment, and IoT systems [67]. Therefore, when executing digital investigations in a smart home, investigators need to deal with data on the local memory of various kinds of smart home devices, phones, and PCs, which are in the scope of devices level forensics. Movement or location information can be extracted from devices with global positioning system (GPS) sensors, accelerometers, gyroscope, and rotation sensors while presence and event data or duration information can be inferred from cameras detection, temperature sensors, or activity sensors [63]. Smart home devices can construct

TABLE II
FORENSIC INVESTIGATION MODELS IN IoT PARADIGM

Forensic Model	Description	Digital Forensic Readiness	Digital Forensic Process
[2]	proposed 1-2-3 zones approach and Next-Best-Thing TRIAGE model for IoT-related forensic investigations.		use 1-2-3 zone and NBT models to instruct evidence identification.
[22]	proposed a top-down forensic model covering the beginning of an standard investigation procedure till the evidence to be archived.	obtain authorization and make plans.	introduce identification of M2M communication and triage examination to the general digital forensic process.
[26]	proposed a forensic framework for CPCS with pre-defined forensic principles.	highlight the need for forensic readiness to collect and preserve information prior to a security incident.	integrate six factors of forensic requirements into the design and development of CPCS.
DFIF-IoT [27]	proposed a generic framework that complied with the international standards, including proactive and reactive processes.	proactive process aims to achieve forensic readiness. It combines FAIoT model with LoS and NBT model.	IoT forensics consists of device level forensics, network forensics, and cloud forensics.
FSAIOT [41]	proposed a general solution to IoT devices state acquisition without physically accessing the device memory and pointed out that IoT device state or the change of state could be of forensic value.	acquire state data from devices, cloud, and hubs.	analyze the log files that include the states and changes of devices to extract findings.
[37]	proposed Last-on-Scene(LoS) algorithm for evidence acquisition that investigators should deal with the last device in the communication chain first.		start forensic process with the last device in the communication chain based on a multi-zone process flow.
[1]	proposed an application-specific IoT forensic model to guide investigation in specific IoT applications.		the model consists of application-specific forensics, digital forensics and forensic process. Data may flow from "application-specific forensic" to "digital forensics" and form into evidence through "forensic process".
IDFIF-IOT [65]	extended DFIF-IoT by considering the interconnection, interoperability and smarter functionality between IoT devices/services and it helped with the integration of IoT standards and protocols with the forensic process.	pre-define the "Things" and take device connectivity and communication networks into consideration to help gathering, storage and handling of digital evidence for digital forensic readiness.	base on DFIF-IoT and is guided by IoT standards and protocols.

a local network using ZigBee and other wireless protocols. These devices, phones and PCs, and cloud can communicate with others via the Internet. Therefore, network forensics is of great value in IoT forensics. Additionally, given that most application data of the smart home is processed and stored in clouds, cloud forensics needs to be carried out.

The main sources of evidence in a smart home consist of devices, networks, and clouds, which also compose the sources of evidence in other IoT forensic scenes. Therefore, IoT forensics can be identified as a combination of cloud forensics, network forensics, and device level forensics. Although sources of evidence may vary with different IoT-based forensic scenes, the investigators need to take all three types into consideration.

1) Device Level Forensics: An investigator may need to collect data from the local memory of various kinds of devices in an IoT scene. Videos and images from closed-circuit television (CCTV) cameras and audio from Amazon Echo are good examples of digital evidence residing at the device level to track the movement activities or behaviors of target entities. Examples of devices include but are not limited to sensors, medical implants, smart meters, smart home appliances, cameras, networked vehicles, RFIDs, and drones.

2) Network Forensics: Different devices, companion clients and the cloud can communicate via various wired or wireless network protocols, which forms the networking and data communication layer of IoT. IoT-related network may utilize one or more types of networks, such as body area network (BAN), personal area network (PAN), home/hospital area networks (HANs), local area networks (LANs), and wide area networks (WANs). For each type of network, there needs to be appropriate methods of forensics after an incident. The data collected at the network level regarding network logs, the flow of data, and routing, which can act as crucial pieces of evidence to condemn or exonerate a suspect [8].

3) Cloud Forensics: Data generated from the IoT devices and IoT networks are usually stored and processed in the cloud. Therefore, cloud forensics plays an important role in the IoT forensics domain. Client-centric artifacts, such as history logs, temp data, registry, access logs, chat logs, session data, and persistent cookies, can be found on the Web browser and Apps. System logs, application logs, user authentication and access information, and database logs can be extracted from the cloud.

Relevant data from various sources of evidence needs to be chained together to reconstruct the case as far as possible.

However, the scope of the data sources cannot be fully determined *a priori* and new sources of evidence may be discovered during the investigation. Therefore, evidence identification is an iterative process.

On the other hand, besides the information extracted from the IoT devices, network, and cloud, behaviors of particular target IoT devices can also act as evidence to prove or disprove the fact. Most IoT devices are composed of various kinds of sensors (e.g., motion sensor, temperature sensor, and light sensor), which may more conclusively prove the location of target individuals or their behaviors. Whether the smart lighting is on or off and the door is locked or unlocked can provide circumstantial evidence to indicate the presence of the individual. The accelerometer within the smart wearable device can refute that the individual was actually awake and also mobile when he/she originally claimed that they were asleep. A smart meter on the scene may show that 140 gallons of water had been used between 1:00 A.M. and 2:00 A.M. on the day of the incident, which may reveal the individual had activities using a large amount of water at that time [43]. These examples demonstrate the importance of IoT device's behaviors as potential sources of evidence in an investigation.

However, as evidence may be dispersed in multiple locations across all these three domains, it is necessary to perform digital investigations with collaboration between different jurisdictions, which may raise challenges with respect to multi-jurisdictional legal issues [30], [68]. When collecting evidence from the device running in a multitenancy environment (e.g., cloud), service providers might be reluctant to allow external parties to access data, so that the investigation may be limited to network and device data that are physically accessible [38]. It may also be impossible to physically hold and extract the evidence from some OOFIs in an IoT environment (e.g., implantable medical devices), so that investigators would need to find alternative data sources.

B. Research on Potential Data Sources in IoT

There are some forensic methods aiming to provide guidelines for identifying artifacts of forensic value in different IoT application scenarios. This kind of work reveals potential sources of forensic interests and explores which kinds of evidence can be obtained from the sources.

Do *et al.* [43] revealed the forensic value of temporal information in smart devices, which may corroborate other findings in legal investigations. They undertook the collection and analysis process on two IoT devices, smart light and smart switch, under two kinds of forensic adversaries (passive adversary and active adversary). The findings show that even the passive forensic adversary (i.e., eavesdroppers) can obtain a variety of forensic-interested data, which can be used to determine the actions and/or presence of an individual. Note that this article classifies the potential information that can be obtained from smart home devices by adversaries with various abilities (from the perspectives of both forensics and malicious attackers). Ryu *et al.* [58] provided a brief description of data acquisition, classification and analysis process of smart home devices, and also analyzed the attack scenarios of collected data and some forensic models suitable for such scenarios.

In most smart home scenarios, heterogeneous devices may connect to a hub, transferring interaction information, temperature or moisture information and some other valuable information. Awasthi *et al.* [44] focused on various types of available information from smart hubs for law enforcement agencies. They investigated Almond+ ecosystem, including the home hub, iOS/Android companion Apps, and cloud environment, to provide forensic examiners with methods of evidence collection and analysis. Changes in humidity, temperature, and motion, and dimming lights can provide a wealth of information about the events. Local-based and cloud-based logs, as well as information from applications, can also act as evidence to describe activities of connected devices and users.

Most smart home devices have companion Apps on mobile phones or laptops for ease of use and control. Dorai *et al.* [62] conducted a forensic analysis on the Nest devices and their companion Apps. They leveraged open-source tools to automatically acquire digital evidence from companion Apps on the devices that are used to control Nest IoT platforms. Their work mainly focused on evidence extraction on the client side. However, the cloud server for smart appliances is also a rich data source. It is worth noting that if the smart hub is rebooted or powered off, valuable digital evidence will be irretrievably lost [44]. Therefore, forensic requirements need to be considered at design time for smart home systems to provide proactive forensic data collection and store the data in the cloud.

Al-Kuwari and Wolthusen [11] proposed a live forensic approach that demonstrated the feasibility of obtaining passenger's behaviors by analyzing intelligent vehicle communication systems. The intelligent vehicle is a rich source of evidence where most driver/passenger comfort and convenience functions, such as telematics, parking assist, and adoptive cruise control (ACC), use multimedia sensors to capture the information of surroundings. Some other sensors, like seat occupant sensors and hands-free phone systems, can be used for driver/passenger identification, and navigation systems can maintain historical records for previous destinations.

Van der Knijff [16] focused on control systems and analyzed possible sources of evidence and their prioritization in a control system. There are two primary sources of evidence in control systems, including the data stored in devices and the data flowing through networks. However, the diversity in control system components may pose challenges to developing forensic acquisition tools. Sohl *et al.* [23] also explored forensics in control systems and mainly focused on forensics in smart grid. They claimed that the evidence acquisition from field devices, i.e., programmable logic controllers (PLCs), intelligent electronic devices (IEDs), phasor measurement units, and smart meters, may not be conducted on the device itself. Data acquisition from a control system is first attempted by running code on the control system to have memory imaging. Bajramovic *et al.* [28] researched smart

TABLE III
SOURCES OF EVIDENCE IN DIFFERENT IoT APPLICATION SCENARIOS

Application Scenarios	Research	Sources of Evidence
Smart home	[43], [58] [44], [62]	smart appliances smart hub Apps on the smartphones or web cloud server local networks
Smart vehicle	[11]	GPS systems, automotive sensors automotive networks and bus systems advanced automotive applications
Control system	[16], [23], [28]	field devices system logs control system networks
Wearables	[59]	wearable device Apps on smartphones and PCs device communication data cloud service
Cloud-enabled IoT devices	[33]	computer hard drive and memory client and web applications

building forensics and highlighted the importance of log data in smart buildings that documents any event that modifies a system's state. The log data offers a thorough record of step-by-step events that happened in a system. For example, an event log is produced when a system in a smart building starts running, stops, or fails to start. Additionally, system logs in smart buildings must be kept secure and tamper-proof to ensure the admissibility of evidence in court.

Teing *et al.* [33] provided a systematic approach for collection and analysis of data artifacts from BitTorrent Sync p2p cloud storage services, which can be used in investigating other BitTorrent-Sync-enabled clients. They revealed that artifacts, such as data files, login credentials, network information, and cloud synchronization metadata, can be recovered by memory dump.

Kasukurti and Patil [59] analyzed in detail the forensic value of wearable devices. Data collected from these devices, such as geo-location information, physical and health information of the user, logs of activities, account details of social media, calendar details, media files, key generation mechanisms, and key-gen logs, can be potential evidence.

In the IoT environment, sources of evidence vary greatly with different forensic scenes, such as home appliances, medical systems, and networked vehicles, where investigators have different focus areas [69]. The main sources of evidence in the main IoT application scenarios are summarized in Table III.

VII. IoT Forensics From the Technical Dimension

Digital forensic investigations rely on scientifically proven forensic methods and validated tools used by qualified forensic experts. A forensic toolkit should be kept ready for forensic investigations to acquire and parse the structured and unstructured data for each encountered data source in a forensically sound manner.

In a smart home scene, investigators can use forensic tools, such as Cellebrite UFED Physical Analyzer and Paraben Device Seizure, to acquire and analyze data from smartphones or tablets. These devices usually use well-understood operating systems such as Android, iOS, or Windows. Investigators can also use CAINE, EnCase, Bulk Extractors, and some other tools to extract card numbers, email addresses, Web addresses, and telephone numbers from the disk images and directory files of PCs while using NetAnalysis and Wireshark for network forensics to parse different network protocols (e.g., ZigBee and Z-wave in the smart home scene). When dealing with some smart appliances, investigators can also use JTAG techniques to access the memory content by connecting special cables to the provided pins on the device or use chip-off techniques when the device is physically broken or locked. Since most IoT data are stored and processed in the cloud with unknown physical locations, investigators also need to extract data from the decentralized and distributed cloud environment. This process may usually be conducted with the help of the cloud service provider. Data extraction from various sources may need to use specific techniques (e.g., reversing techniques) to bypass access control, encryption, and some other security mechanisms.

In this section, we review enabling techniques for IoT forensics, mainly including evidence extraction techniques, forensic readiness techniques, and some other forensic techniques.

A. Evidence Extraction Techniques

Evidence extraction in IoT environment requires a wide range of tools and techniques across multiple digital forensic branches, including computer forensics, mobile forensics, and embedded forensics for working with local storage; network forensics for accessing and analyzing the communications medium; and cloud forensics for analyzing the remote storage [46].

Although there are some digital forensic tools that are applicable to some data sources in IoT environment, there is also a lack of appropriate tools to derive meaningful content from some specific IoT devices, for example, RFID-based devices. These devices usually rely on flash memory with no built-in file system storage capability, which may not be readable or accessible with existing tools. Toldinas *et al.* [70] analyzed the suitability of existing forensic tools for investigations in IoT and highlighted that existing traditional computer forensic tools are insufficient for IoT forensics. Additionally, it is common that the same kind of IoT products from different manufacturers may have different hardware platforms, operating systems, or filesystem formats, which pose a challenge to developing forensics tools for heterogeneous devices. This is now a significant area of concern with research efforts to extract data from heterogeneous IoT devices in a forensically sound manner. We then discuss the research on collecting forensic data from various kinds of data sources in IoT environment, including smart devices, network, and cloud.

Some research focuses on reverse engineering of CCTV systems or digital video recorder (DVR) systems to extract available videos and its metadata for digital forensic investigations. Tobin *et al.* [17] dealt with recovering and interpreting data from the disk image of a CCTV system with a proprietary file system. The method can provide a map to indicate where the video data resides, helping investigators to easily understand where data is located on the disk. But this approach failed to interpret the video data. For future development, they try to provide more detailed analysis on the CCTV system to allow for the viewing of this video data. Park and Lee [18] proposed a method to extract meaningful information from video data fragments related to DVRs. Their method consists of five steps: 1) preprocessing; 2) classification; 3) reassembly; 4) extraction; and 5) postprocessing. A playable video file will be constructed based on metadata stored in video frames, such as timestamp, GPS location, camera number, or speed.

Boztas *et al.* [20] explored collection of evidence from smart TVs. Most smart TVs contain a camera, microphones, and a management platform that allows users to install applications and visit Websites. Using some data acquisition methods (e.g., eMMC five-wire method and NFI Memory Toolkit II), investigators can acquire data from the flash memory of TVs (e.g., an eMMC chip) to obtain Web browsing records, photo and multimedia files, external media (e.g., USB flash drive), cloud services, and channel record. They can also trace the interaction information (e.g., connected devices, network information, and smart functions) from system information and settings.

Kang *et al.* [60] explored obtaining evidence from wearable devices. They focused on two popular fitness trackers: 1) Xiaomi Mi Band 2 and 2) Fitbit Alta HR, and explored the forensic analysis methods for files on the devices. Horsman [24] discussed how to recover flight data from the internal storage of both UAVs and their controlling devices.

Shin *et al.* [38] investigated available approaches, such as eMMC Root, JTAG, and debug ports, to extract potential evidence from several widely used IoT devices, such as Amazon Echo, Z-wave devices, and home routers. Bharadwaj and Singh [40] proposed a proof-of-concept tool, called RIFT, which aims at acquisition and preservation of forensically relevant artifacts from the Raspberry Pi-IoT platform.

Since most IoT devices may have proprietary interfaces and storage units, and IoT networks are also highly heterogeneous with various network protocols, it may be promising to standard the markets to develop general solutions for performing routine forensic tasks in IoT environment. On the other hand, although specialized tools and techniques are gradually being developed to extract and interpret the contents from specific systems, the reliability of tools and techniques needs to be verified. The data collection process itself may produce incorrect information intermingled with data, which may compromise the integrity of data [5].

Besides device-level data acquisition techniques, network forensics techniques and methodologies are also key enablers for IoT forensics. Different from acquiring data from traditional storage media, various kinds of networks with unpredictable communication channels (e.g., ad hoc networks) pose great challenges to IoT forensics. It may lead to dynamic changes in network environment that IoT devices can move with people crossing different networks. Kumar *et al.* [19] presented an approach that correlated RAM and flash contents from sensor nodes to extract network connectivity information to reconstruct the network topology. They also developed a forensic tool to analyze RAM dumps from the devices using Contiki OS.

IoT devices may use non-IP protocols when communicating with proximal devices located on BAN, PAN, or LAN, while using IP network when communicating with cloud service providers. Most hardware used in networks records transmitted data itself or some other information about that data in logs. These logs are indispensable to forensic investigators as they may contain valuable information for the investigation. Investigators need to understand various kinds of communication protocols to extract and analyze data from network traffic. However, contemporary digital forensic schemes, tools, and technologies may not be able to deal with the properties of each communication protocol encountered in IoT forensics [51]. On the other hand, regardless of which form of network is used, most data in networks is volatile. Volatile data should be given priority over nonvolatile data.

Cloud plays a great role in sources of evidence in IoT environment because most IoT data is processed, stored, and analyzed in the cloud. Although current studies on IoT forensics are in their very early stages, there are some successful models helping evidence acquisition from the cloud [71]–[73]. Investigators need to extract system logs, application logs, user authentication and access information, database logs, and other important information from the cloud to assist IoT forensics.

Additionally, encryption is a foundation for information security while thwarting forensic investigations. The conflict between information security and force decryption for forensics still remains in IoT forensics. Accessing encrypted data on Apple or Android devices or clouds may need to seek legal remedies.

B. Forensic Readiness Techniques

Different from traditional digital forensic scenes where the examiner can hold the digital equipment to acquire evidence, in some IoT cases it may be impractical to isolate and shut down some devices and take them back to the laboratory for evidence extraction [26]. For instance, if the VM instances are forcibly shut down, the volatile data of forensic interest will be lost, influencing the event reconstruction. Therefore, it is necessary for IoT forensics to proactively collect and preserve valuable data of forensic interest to enhance the forensic ability of the environment and minimize the cost for incident responses [74]. Some research explores the forensic readiness system to collect evidence from IoT systems in real time and then send evidence to a trusted repository for storage, which can ensure the forensic ability in an IoT environment.

1) General Forensic Readiness System: Zawoad and Hasan [21] proposed a centralized trusted evidence repository that provides secure evidence repository service to all registered IoT devices that are applied with the secure logging scheme [75]. It also applies secure provenance chaining [76] to preserve the integrity of the access history of the evidence. The centralized repository helps to deal with heterogeneity and scalability challenges of digital forensics within an IoT environment.

Kebande *et al.* [35] proposed a cloud-centric conceptual framework for isolating big data evidence from an IoT-based environment. The framework consists of a cloud/IoT infrastructure layer, a forensic evidence isolation layer, and a digital forensic investigation layer. The cloud/IoT infrastructure layer is responsible for collecting interconnection data between different devices via lightweight wireless protocols like ZigBee and Z-wave. The forensic evidence isolation layer aims to find the root cause of an incident in the cloud by virtual instance isolation. These two layers focus on providing forensics preparation before an incident happens. The digital forensic investigation layer is a post-event response process for forensic investigations.

Babun *et al.* [77] presented IoTDots to collect, store, and process smart environment data that can be used for later investigations. IoTDots can extract forensically relevant logs from smart Apps and automatically analyze the logs if necessary. It consists of two components: IoTDots-Modifier and IoTDots-Analyzer. Modifier can analyze the smart Apps' source code and insert specific logging statements at compile time, and runtime logs will be sent to the cloud for preservation. Analyzer is responsible for extracting valuable forensic information from logs using machine learning techniques. However, the transfer of artifacts may increase network traffic, affecting service availability in some wireless networks (e.g., 6LoWPAN).

ProvThings [78] is a general and platform-centric approach providing a holistic explanation of system activities (include malicious behaviors). It uses a set of collectors to track data flow and method invocation, and then merges provenance records from different components of an IoT platform to generate provenance data. Experiments demonstrated that ProvThings can provide provenance for a corpus of 26 known IoT attacks, which assists with efficient investigations and system diagnosis.

Besides preserving case-related data on the devices, there are also research efforts focusing on collecting network traffic data. However, wide varieties of network protocols for IoT limit the availability of existing forensic readiness frameworks [8]. In addition, existing work on traffic forensics has predominantly relied on introducing additional powerful forensic nodes (i.e., sniffer nodes) to capture and forward sensor node behaviors information. By collecting behavior information of nodes, Kumar *et al.* [25] have proposed a traffic analysis tool that can identify the attacks in 6LoWPAN.

Probe-IoT [51] and FIF-IoT [50] are two models using blockchain technology to acquire and preserve evidence in IoT-based systems. They provide a tamper-evident scheme to store evidence in a trustworthy manner. They use the digital ledger to maintain a track record of all the transactions in an IoT-based system, including transactions between things and users, between things and cloud, and between things to things. Due to the nature of blockchain, Probe-IoT and FIF-IoT can ensure the confidentiality, anonymity, and nonrepudiation of publicly available evidence.

Al-Masri *et al.* [49] introduced a fog-based IoT forensic framework that can identify and mitigate cyber-attacks on IoT systems at early stages. The effectiveness of the framework needs to be further evaluated.

2) Application-Specific Forensic Readiness System: Oriwoh and Sant [14] designed a system that can be integrated into a smart home network to provide automated forensic services and basic security services. The system proactively collected and stored the network data and predefined some security events that can trigger the reactive forensics responses. Chung *et al.* [31] focused on recovering forensic artifacts from IoT systems, including data on the device and on the cloud. They proposed a forensic framework to collect and analyze forensic data in an Amazon Alexa ecosystem to confirm or disprove a user's involvement in criminal behavior.

Ellouze *et al.* [32] proposed a digital investigation system that integrates a library of medical rules for the postmortem analysis of lethal attack scenarios on cardiac implantable medical devices. It recorded and stored logs as digital evidence to automatically infer potential medical scenarios and track sensitive events.

Hossain *et al.* [36] proposed a trustworthy forensic framework for the distributed Internet of Vehicles (IoV) infrastructure that can collect and preserve trustworthy evidence. Trust-IoV provides a secure provenance of the evidence to ensure its integrity, which helps investigators to verify the integrity of the evidence during an investigation in highly distributed smart vehicle-based environment. Feng *et al.* [34] focused on forensics in smart vehicles. They investigated and analyzed the threats to smart vehicles in a smart city. However, the proposed model is in infancy, that needs to be validated in a real scenario. Hussain *et al.* [52] proposed a new concept that vehicles moving on the road could be employed as witnesses to the designated event. They designed a forensics framework to detect the occurrence of the designated events on the road. When confronted with an event, the vehicles in the vicinity with mounted cameras can collaborate with other roadside cameras to take pictures of the site of interest around them and send the pictures to the cloud infrastructure anonymously.

C. Other Forensic Techniques and Methodologies

1) Data Reduction: The increasing number of IoT devices increases the volume of forensic data. Investigators have to go through hundreds and thousands of structured or unstructured documents gathered from data sources to extract and assess relevant pieces of information.

Some research explored the selective imaging method to reduce the volume of forensic data and to automatically extract relevant data, whilst retaining information in the native source file format with original metadata [79], [80]. There is also some work using data mining and machine learning methods to efficiently identify the facts from big digital forensic data [61], [81]. However, results obtained from these techniques are usually hard to interpret, which leads to doubt whether the results are reliable and legally acceptable.

2) Correlation Analysis: Merging data from a variety of data sources can assist to provide a greater understanding of a corpus of data [82]. Although analyzing a variety of disparate devices is not new to digital forensic analysis, it is becoming more difficult to completely identify all sources of evidence when the boundary of an IoT-based case is blurry. There is also a challenge to keep balance between the growing volume of data and time cost in IoT forensic paradigm [47].

Quick and Choo [55] explored the cross-device and cross-case analysis method and quick analysis techniques. They proposed a semiautomated scanning method for disparate forensic data subsets, including data from a variety of portable devices, computers, mobile phones, and the cloud.

3) Timeline Reconstruction: The time parameter is of great value for the association of evidence from different sources and helps to sequence the relevant incidents of interest. However, many devices are not time-synchronized because they use different time granularities and users are spread over different time zones, which increases the complexity of timeline reconstruction for IoT forensics [83].

Inglot *et al.* [12] reviewed a timeline analysis tool, Zeitline, and discussed its shortcomings. They also outlined promising improvements to enhance the timeline analysis function of Zeitline for IoT forensics.

4) Trustworthiness of Data: Since malicious data can be inserted into the raw data and data in transmission can be altered by the owner or a third party hacker, there is doubt about how much we can trust the data extracted from IoT devices [84].

Nieto *et al.* [6] provided a preliminary analysis of security guarantees for data on personal IoT devices. They proposed that embedded secure architectures can be used to construct trusted execution environment and hardware-based anti-tampering solutions can provide proof of the integrity of the digital evidence on the devices.

5) Privacy Concern: Data stored and processed on IoT devices may be sensitive. To collect and analyze data on some IoT devices, investigators may access the sensitive data, which raises privacy concern. Existing work has already started to focus on privacy preservation in the investigation process. Nieto *et al.* [85] proposed privacy-aware IoT-forensics to integrate privacy properties with the forensic model adapted to IoT, which lays the groundwork for voluntary cooperation in cybercrime investigations. Doubt remains whether digital investigators have the right to view everything on devices of interest. Therefore, the digital investigation process needs to find a balance between privacy concerns and the possibilities for law enforcement.

VIII. Open Issues and Suggestions

In this section, based on our observation from surveying the research achievements in the field of IoT forensics, we highlight open issues in the context of IoT forensics and put forward promising suggestions from three dimensions.

From the temporal dimension, IoT forensics needs to perform a standard investigation process to handle evidence in a forensically sound manner. Current research efforts in IoT forensic models are in their early stages without full implementation in practical cases. There is a pressing need for appropriate models that can provide accepted guidance and principles to perform routine forensic tasks in IoT environment. Although the digital forensic process model is not standardized, there exists a consensus that the IoT forensic model still follows the four-phase forensic process. We have several suggestions for developing standard IoT forensic models.

1) For the collection process, it is critical to preserve and collect the evidence by priority with the consideration of volatility, difficulty, and value of data. For example, volatile data should be given priority over nonvolatile data. So first responders must carefully decide whether to turn off the device to preserve the data or to preserve the evidence on the devices by transferring data from the scene to a remote server to reduce the damage to the evidence as much as possible. Dividing the data sources into logical domains may simplify the complexity and speed up the process in parallel.
2) For examination and analysis processes, investigators need to use a methodical approach to deal with the data and combine the data from different data sources. It might be necessary to standardize data storage formats and interfaces on similar kinds of devices to extract and analyze evidence effectively, which can also help to standardize the market.
3) For the reporting process, investigators need to prepare highly detailed reports of all information gathered and present the information in appropriate manners so that both a technical investigator and a layperson, such as judge, jury and the parties involved, can understand.

From the spatial dimension, considering the three-tier architecture of IoT, the forensic process in IoT environment may necessitate all three levels including device level forensics, network forensics, and cloud forensics. Evidence from different data sources can be complementary to prove or disprove plausible explanations. New data sources may appear constantly in IoT forensic environment, calling for appropriate forensic solutions. To deal with various types of data sources in IoT forensics environment, we point out some suggestions as follows.

1) From the device level forensics, investigators need to carefully verify the integrity of data from various kinds of heterogeneous devices that may lack adequate security mechanisms. Additionally, particular behaviors of target devices also create another venue for forensic investigations.
2) From the network forensics, it is necessary to develop toolkits to parse different network protocols widely used in different types of IoT networks. Most data in networks is volatile, and may need to be selectively preserved or documented in advance to speed up the forensic process.
3) From the cloud forensics, digital forensics-as-a-service is recommended to be integrated into the cloud to provide secure provenance for forensics.
4) Investigators should be aware of the range of possible data sources and use alternative data sources when the primary source is unavailable.

From the technical dimension, existing tools or methods may be insufficient to deal with some unique challenges in IoT forensics. We highlight some suggestions on exploring innovative tools and techniques to enhance digital forensic capabilities.

1) Due to diverse and ever-changing networks and automatic execution in IoT, there is a strong need for valid forensic readiness systems equipped in the design of IoT systems to capture real-time logs and store them

in a valid uniform form, maximizing an environment's forensics ability and minimizing the cost of forensics.

2) To deal with various kinds of data sources, existing tools and techniques across multiple digital forensics branches, such as computer, mobile, network, and embedded forensics, can be tailored to IoT environment. If the existing tools do not work, customized tools for special situations need to be carefully assessed prior to their use.
3) It is promising to promote the existing forensics methods with the help of some other evolving techniques, such as machine learning and natural language processing, which behaves well in analysis and classification of a large volume of data and modeling of human behaviors. For example, deep learning is widely used to identify human faces and voices from photos or videos and side channel techniques to identify devices from wire and wireless communication.

Furthermore, IoT forensics needs to be in compliance with laws and regulations that pertain to the investigation. Although current legal systems may still be largely applicable to IoT forensics, digital investigations in the age of IoT call for additional legislation. Laws and regulations need to keep pace with the involvement of technologies and forensic procedures in the context of IoT, concerning responsibility attribution, multijurisdiction collaboration, privacy concerns, anti-forensics, and so on.

IX. Conclusion

The fundamental characteristics of IoT have had a great impact on traditional digital forensics. Ubiquitous sensing increases the amount, sources and diversity of potential evidence. Dynamic changes make it more difficult to identify entities involved and demarcate the boundary of a case. Automated execution raises the complexity of deciding who is in charge and who should be blamed. The resource-limited characteristic makes it hard to locate and seize volatile or nonvolatile data from IoT environment. Heterogeneity significantly increases the workload of investigators. The special security nature of IoT may cause the concern of removing and modifying potential evidence.

The increased public awareness of IoT forensics leads to a sharp increase in studies on it. To have a better overview of research directions and state of research in this domain, we sketch the landscape of IoT forensics under a 3-D framework, which comprises a spatial dimension, a temporal dimension, and a technical dimension. We take the smart home as an example to illustrate IoT forensics from the three dimensions. Under the 3-D framework, we thoroughly review the existing research efforts and we hope that it can provide guidelines for forensic practitioners and researchers. From the temporal dimension, forensic models to instruct forensic investigations in IoT paradigm should follow the basic forensic process and need to be adjusted to accommodate IoT environment in practice. From the spatial dimension, investigators need to gain access to rich sources of potential evidence in the IoT, including devices, networks, and clouds. Evidence from various data sources need to be chained together to reconstruct the scene of an incident. From the technical dimension, new forensic tools/techniques and forensic readiness systems for IoT environment should offer real-time logging, volatile data analysis, and the support of various hardware and file systems to deal with new data sources.

Much effort has been devoted to IoT forensics, but there are still many open issues to face. We summarize the open issues and propose corresponding suggestions from the three dimensions. We hope this article can help to point out the research road ahead for IoT forensics.

References

[1] T. A. Zia, P. Liu, and W. Han, "Application-specific digital forensics investigative model in Internet of Things (IoT)," in *Proc. 12th Int. Conf. Availability Rel. Security*, Reggio Calabria, Italy, Aug./Sep. 2017, pp. 1–7.

[2] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of Things forensics: Challenges and approaches," in *Proc. 9th IEEE Int. Conf. Collaborative Comput. Netw. Appl. Worksharing*, Austin, TX, USA, Oct. 2013, pp. 608–615.

[3] G. Palmer *et al.*, "A road map for digital forensic research," in *Proc. 1st Digit. Forensic Res. Workshop*, Utica, NY, USA, 2001, pp. 27–30.

[4] K. Kent, S. Chevalier, T. Grance, and H. Dang, *Guide to Integrating Forensics Techniques Into Incident Response*, document SP 800–86, Comput. Security Division, Inf. Technol. Lab., Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, 2006. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

[5] R. McKemmish, "When is digital evidence forensically sound?" in *Proc. 4th Annu. Adv. Digit. Forensics IV (IFIP WG)*, Jan. 2008, pp. 3–15.

[6] A. Nieto, R. Roman, and J. López, "Digital witness: Safeguarding digital evidence by using secure architectures in personal devices," *IEEE Netw.*, vol. 30, no. 6, pp. 34–41, Nov./Dec. 2016.

[7] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 78, pp. 544–546, Jan. 2018.

[8] U. Karabiyik and K. Akkaya "Digital forensics for IoT and WSNs," in *Mission-Oriented Sensor Networks and Systems: Art and Science—Volume 2: Advances*, 2019, pp. 171–207.

[9] S. Watson and A. Dehghantanha, "Digital forensics: The missing piece of the Internet of Things promise," *Comput. Fraud Security*, vol. 2016, no. 6, pp. 5–8, 2016.

[10] J. Hou, L. Qu, and W. Shi, "A survey on Internet of Things security from data perspectives," *Comput. Netw.*, vol. 148, pp. 295–306, Jan. 2019.

[11] S. Al-Kuwari and S. D. Wolthusen, "On the feasibility of carrying out live real-time forensics for modern intelligent vehicles," in *Proc. 3rd Int. Conf. Forensics Telecommun. Inf. Multimedia (ICST)*, Shanghai, China, Nov. 2010, pp. 207–223.

[12] B. Inglot, L. Liu, and N. Antonopoulos, "A framework for enhanced timeline analysis in digital forensics," in *Proc. IEEE Int. Conf. Green Comput. Commun. Conf. Internet Things Conf. Cyber Phys. Soc. Comput. (GreenCom/iThings/CPSCom)*, Besancon, France, Nov. 2012, pp. 253–256.

[13] I. Homem, S. Dosis, and O. Popov, "LEIA: The live evidence information aggregator: Towards efficient cyber-law enforcement," in *Proc. World Congr. Internet Security (WorldCIS)*, London, U.K., Dec. 2013, pp. 156–161.

[14] E. Oriwoh and P. Sant, "The forensics edge management system: A concept and design," in *Proc. IEEE 10th Int. Conf. Ubiquitous Intell. Comput. IEEE 10th Int. Conf. Auton. Trusted Comput. (UIC/ATC)*, Dec. 2013, pp. 544–550.

[15] I. Sutherland, H. Read, and K. Xynos, "Forensic analysis of smart TV: A current issue and call to arms," *Digit. Invest.*, vol. 11, no. 3, pp. 175–178, 2014.

[16] R. M. van der Knijff, "Control systems/SCADA forensics, what's the difference?" *Digit. Invest.*, vol. 11, no. 3, pp. 160–174, 2014.

[17] L. Tobin, A. F. Shosha, and P. Gladyshev, "Reverse engineering a CCTV system, a case study," *Digit. Invest.*, vol. 11, no. 3, pp. 179–186, 2014.

[18] J. Park and S. Lee, "Data fragment forensics for embedded DVR systems," *Digit. Invest.*, vol. 11, no. 3, pp. 187–200, 2014.

[19] V. Kumar, G. C. Oikonomou, T. Tryfonas, D. Page, and I. W. Phillips, "Digital investigations for IPV6-based wireless sensor networks," *Digit. Invest.*, vol. 11, no. S-2, pp. S66–S75, 2014.

[20] A. Boztas, A. R. J. Riethoven, and M. Roeloffs, "Smart TV forensics: Digital traces on televisions," *Digit. Invest.*, vol. 12, no. S1, pp. S72–S80, 2015.

[21] S. Zawoad and R. Hasan, "FAIoT: Towards building a forensics aware eco system for the Internet of Things," in *Proc. IEEE Int. Conf. Services Comput. (SCC)*, New York, NY, USA, Jun./Jul. 2015, pp. 279–284.

[22] S. Perumal, N. M. Norwawi, and V. Raman, "Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology," in *Proc. 5th Int. Conf. Digit. Inf. Process. Commun. (ICDIPC)*, 2015, pp. 19–23.

[23] E. Sohl *et al.*, "A field study of digital forensics of intrusions in the electrical power grid," in *Proc. 1st ACM Workshop Cyber Phys. Syst. Security Privacy (CPS-SPC)*, Denver, CO, USA, Oct. 2015, pp. 113–122.

[24] G. Horsman, "Unmanned aerial vehicles: A preliminary analysis of forensic challenges," *Digit. Invest.*, vol. 16, pp. 1–11, Mar. 2016.

[25] V. Kumar, G. C. Oikonomou, and T. Tryfonas, "Traffic forensics for IPV6-based wireless sensor networks and the Internet of Things," in *Proc. 3rd IEEE World Forum Internet Things (WF-IoT)*, Reston, VA, USA, Dec. 2016, pp. 633–638.

[26] N. H. A. Rahman, W. B. Glisson, Y. Yang, and K.-K. R. Choo, "Forensic-by-design framework for cyber-physical cloud systems," *IEEE Cloud Comput.*, vol. 3, no. 1, pp. 50–59, Jan./Feb. 2016.

[27] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," in *Proc. 4th IEEE Int. Conf. Future Internet Things Cloud (FiCloud)*, Vienna, Austria, Aug. 2016, pp. 356–362.

[28] E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, "Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests," in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, Trento, Italy, Sep. 2016, pp. 1–6.

[29] D. Vandervort, "Medical device data goes to court," in *Proc. 6th Int. Conf. Digit. Health Conf. (DH)*, Montreal, QC, Canada, Apr. 2016, pp. 23–27.

[30] Z. A. Baig *et al.*, "Future challenges for smart cities: Cyber-security and digital forensics," *Digit. Invest.*, vol. 22, pp. 3–13, Sep. 2017.

[31] H. Chung, J. Park, and S. Lee, "Digital forensic approaches for Amazon Alexa ecosystem," *Digit. Invest.*, vol. 22, pp. S15–S25, Aug. 2017.

[32] N. Ellouze, S. Rekhis, N. Boudriga, and M. Allouche, "Cardiac implantable medical devices forensics: Postmortem analysis of lethal attacks scenarios," *Digit. Invest.*, vol. 21, pp. 11–30, Jun. 2017.

[33] Y.-Y. Teing, A. Dehghantanha, K.-K. R. Choo, and L. T. Yang, "Forensic investigation of P2P cloud storage services and backbone for IoT networks: Bittorrent sync as a case study," *Comput. Elect. Eng.*, vol. 58, pp. 350–363, Feb. 2017.

[34] X. Feng, E. S. Dawam, and S. Amin, "A new digital forensics model of smart city automated vehicles," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, Exeter, U.K., Jun. 2017, pp. 274–279.

[35] V. R. Kebande, N. M. Karie, and H. S. Venter, "Cloud-centric framework for isolating big data as forensic evidence from IoT infrastructures," in *Proc. 1st Int. Conf. Next Gener. Comput. Appl. (NextComp)*, 2017, pp. 54–60.

[36] M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A trustworthy forensic investigation framework for the Internet of Vehicles (IoV)," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, 2017, pp. 25–32.

[37] M. Harbawi and A. Varol, "An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework," in *Proc. 5th Int. Symp. Digit. Forensic Security (ISDFS)*, 2017, pp. 1–6.

[38] C. Shin, P. Chandok, R. Liu, S. J. Nielson, and T. R. Leschke, "Potential forensic analysis of IoT data: An overview of the state-of-the-art and future possibilities," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, Exeter, U.K., Jun. 2017, pp. 705–710.

[39] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards developing network forensic mechanism for Botnet activities in the IoT based on machine learning techniques," in *Proc. 9th Int. Conf. Mobile Netw. Manag. (MONAMI)*, Melbourne, VIC, Australia, Dec. 2017, pp. 30–44.

[40] N. K. Bharadwaj and U. Singh, "Acquisition and analysis of forensic artifacts from Raspberry Pi an Internet of Things prototype platform," in *Proc. 5th Intell. Comput. Techn. (ICACNI)*, vol. 1, 2017, p. 311.

[41] C. Meffert, D. Clark, I. M. Baggili, and F. Breitinger, "Forensic state acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition," in *Proc. 12th Int. Conf. Availability Rel. Security*, Reggio Calabria, Italy, Aug./Sep. 2017, pp. 1–11.

[42] N.-A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens, and K.-K. R. Choo, "Smart vehicle forensics: Challenges and case study," *Future Gener. Comput. Syst.*, Jun. 2018. [Online]. Available: https://doi.org/10.1016/j.future.2018.05.081

[43] Q. Do, B. Martini, and K.-K. R. Choo, "Cyber-physical systems information gathering: A smart home case study," *Comput. Netw.*, vol. 138, pp. 1–12, Jun. 2018.

[44] A. Awasthi, H. O. L. Read, K. Xynos, and I. Sutherland, "Welcome pwn: Almond smart home hub forensics," *Digit. Invest.*, vol. 26, pp. S38–S46, Jul. 2018.

[45] D. Quick and K.-K. R. Choo, "Digital forensic intelligence: Data subsets and open source intelligence (DFINT+OSINT): A timely and cohesive mix," *Future Gener. Comput. Syst.*, vol. 78, pp. 558–567, Jan. 2018.

[46] M. Chernyshev, S. Zeadally, Z. A. Baig, and A. Woodward, "Internet of Things forensics: The need, process models, and open issues," *IT Prof.*, vol. 20, no. 3, pp. 40–49, May/Jun. 2018.

[47] Á. MacDermott, T. Baker, and Q. Shi, "IoT forensics: Challenges for the IoA era," in *Proc. 9th IFIP Int. Conf. New Technol. Mobility Security (NTMS)*, Paris, France, Feb. 2018, pp. 1–5.

[48] G. Bréda, P. J. Varga, and Z. Illési, "Forensic functional profile of lot devices-based on common criteria," in *Proc. IEEE 16th Int. Symp. Intell. Syst. Informat. (SISY)*, 2018, pp. 261–264.

[49] E. Al-Masri, Y. Bai, and J. Li, "A fog-based digital forensics investigation framework for IoT systems," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, 2018, pp. 196–201.

[50] M. M. Hossain, R. Hasan, and S. Zawoad, "Probe-IoT: A public digital ledger based forensic investigation framework for IoT," in *Proc. IEEE Conf. Comput. Commun. Workshops (IEEE INFOCOM) Workshops*, Honolulu, HI, USA, Apr. 2018, pp. 1–2.

[51] M. M. Hossain, Y. Karim, and R. Hasan, "FIF-IoT: A forensic investigation framework for IoT using a public digital ledger," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, San Francisco, CA, USA, Jul. 2018, pp. 33–40.

[52] R. Hussain *et al.*, "Secure and privacy-aware incentives-based witness service in social Internet of Vehicles clouds," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2441–2448, Aug. 2018.

[53] V. R. Kebande, S. Malapane, N. M. Karie, H. S. Venter, and R. D. Wario, "Towards an integrated digital forensic investigation framework for an IoT-based ecosystem," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, 2018, pp. 93–98.

[54] M. B. Al-Sadi, L. Chen, and R. J. Haddad, "Internet of Things digital forensic investigation using open source gears," in *Proc. IEEE SoutheastCon*, 2018, pp. 1–5.

[55] D. Quick and K.-K. R. Choo, "IoT device forensics and data reduction," *IEEE Access*, vol. 6, pp. 47566–47574, 2018.

[56] S. Alabdulsalam, K. Schaefer, M. T. Kechadi, and N.-A. Le-Khac, "Internet of Things forensics—Challenges and a case study," in *Proc. 14th IFIP WG Int. Conf. Adv. Digit. Forensics XIV*, New Delhi, India, Jan. 2018, pp. 35–48.

[57] M. S. G. Devi and M. J. Nene, "Security breach and forensics in intelligent systems," in *Information and Communication Technology for Intelligent Systems*, vol. 2, 2018, p. 349.

[58] J. H. Ryu, S. Y. Moon, and J. H. Park, "The study on data of smart home system as digital evidence," in *Proc. CSA/CUTE*, 2017, pp. 967–972.

[59] D. H. Kasukurti and S. Patil, "Wearable device forensic: Probable case studies and proposed methodology," in *Proc. Int. Symp. Security Comput. Commun.*, 2018, pp. 290–300.

[60] S. Kang, S. Kim, and J. Kim, "Forensic analysis for IoT fitness trackers and its application," *Peer-to-Peer Netw. Appl.*, pp. 1–10, Dec. 2018. [Online]. Available: https://link.springer.com/article/10.1007/s12083-018-0708-3

[61] G. S. Chhabra, V. P. Singh, and M. Singh, "Cyber forensics framework for big data analytics in IoT environment using machine learning," *Multimedia Tools Appl.*, pp. 1–20, Jul. 2018. [Online]. Available: https://link.springer.com/article/10.1007/s11042-018-6338-1

[62] G. Dorai, S. Houshmand, and I. M. Baggili, "I know what you did last summer: Your smart home Internet of Things and your iPhone forensically ratting you out," in *Proc. ACM 13th Int. Conf. Availability Rel. Security*, 2018, p. 49.

[63] F. Bouchaud, G. Grimaud, and T. Vantroys, "IoT forensic: Identification and classification of evidence in criminal investigations," in *Proc. 13th Int. Conf. Availability Rel. Security (ARES)*, Hamburg, Germany, Aug. 2018, pp. 1–9.

[64] M. M. Losavio, K. Chow, A. Koltay, and J. James, "The Internet of Things and the smart city: Legal challenges with digital forensics, privacy, and security," *Security Privacy*, vol. 1, no. 3, p. e23, 2018.

[65] A. Nieto, R. Rios, and J. López, "IoT-forensics meets privacy: Towards cooperative digital investigations," *Sensors*, vol. 18, no. 2, p. 492, 2018.

[66] *Information Technology—Security Techniques—Incident Investigation Principles and Processes*, ISO/IEC Standard 27043:2015, 2015. [Online]. Available: https://www.iso.org/standard/44407.html

[67] E. Casey, "Editorial—A sea change in digital forensics and incident response," *Digit. Invest.*, vol. 17, pp. A1–A2, Jun. 2016.

[68] J. I. James and P. Gladyshev, "A survey of mutual legal assistance involving digital evidence," *Digit. Invest.*, vol. 18, pp. 23–32, Sep. 2016.

[69] N. Akatyev and J. I. James, "Evidence identification in IoT networks based on threat assessment," *Future Gener. Comput. Syst.*, vol. 93, pp. 814–821, Apr. 2019. [Online]. Available: https://doi.org/10.1016/j.future.2017.10.012

[70] J. Toldinas, A. Venčkauskas, Š. Grigaliūnas, R. Damaševičius, and V. Jusas, "Suitability of the digital forensic tools for investigation of cyber crime in the Internet of Things and services," in *Proc. RCITD*, 2015, pp. 86–97.

[71] A. Pichan, M. Lazarescu, and S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," *Digit. Invest.*, vol. 13, pp. 38–57, Jun. 2015.

[72] K.-K. R. Choo, C. Esposito, and A. Castiglione, "Evidence and forensics in the cloud: Challenges and future research directions," *IEEE Cloud Comput.*, vol. 4, no. 3, pp. 14–19, 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7962121

[73] C. Liu, A. Singhal, and D. Wijesekera, "Identifying evidence for cloud forensic analysis," in *Proc. 13th IFIP WG Int. Conf. Adv. Digit. Forensics XIII*, Orlando, FL, USA, Jan./Feb. 2017, pp. 111–130.

[74] M. Elyas, A. Ahmad, S. B. Maynard, and A. Lonie, "Digital forensic readiness: Expert perspectives on a theoretical framework," *Comput. Security*, vol. 52, pp. 70–89, Jul. 2015.

[75] S. Zawoad, A. K. Dutta, and R. Hasan, "SecLaaS: Secure logging-as-a-service for cloud forensics," in *Proc. 8th ACM Symp. Inf. Comput. Commun. Security (ASIA CCS)*, Hangzhou, China, May 2013, pp. 219–230.

[76] R. Hasan, R. Sion, and M. Winslett, "The case of the fake Picasso: Preventing history forgery with secure provenance," in *Proc. 7th USENIX Conf. File Storage Technol.*, San Francisco, CA, USA, Feb. 2009, pp. 1–14.

[77] L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, "IoTDoTs: A digital forensics framework for smart environments," *arXiv preprint arXiv:1809.00745*, pp. 1–15, 2018. [Online]. Available: http://arxiv.org/abs/1809.00745

[78] Q. Wang, W. U. Hassan, A. M. Bates, and C. A. Gunter, "Fear and logging in the Internet of Things," in *Proc. 25th Annu. Netw. Distrib. Syst. Security Symp. (NDSS)*, San Diego, CA, USA, Feb. 2018, pp. 1–15.

[79] D. Quick and K.-K. R. Choo. (2014). *Data Reduction and Data Mining Framework for Digital Forensic Evidence: Storage, Intelligence, Review and Archive*. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2497796

[80] D. Quick and K.-K. R. Choo, "Big forensic data reduction: Digital forensic images and electronic evidence," *Clust. Comput.*, vol. 19, no. 2, pp. 723–740, 2016.

[81] H. J. Mohammed, N. L. Clarke, and F. Li, "Evidence identification in heterogeneous data using clustering," in *Proc. 13th Int. Conf. Availability Rel. Security (ARES)*, Hamburg, Germany, Aug. 2018, p. 35.

[82] C. Lin, L. Zhitang, and G. Cuixia, "Automated analysis of multi-source logs for network forensics," in *Proc. IEEE 1st Int. Workshop Educ. Technol. Comput. Sci.*, 2009, pp. 660–664.

[83] Y. Chabot, A. Bertaux, C. Nicolle, and M.-T. Kechadi, "A complete formalized knowledge representation model for advanced digital forensics timeline analysis," *Digit. Invest.*, vol. 11, no. S-2, pp. S95–S105, 2014.

[84] Q. Do, B. Martini, and K.-K. R. Choo, "A data exfiltration and remote exploitation attack on consumer 3D printers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 10, pp. 2174–2186, Oct. 2016.

[85] A. Nieto, R. Rios, and J. López, "A methodology for privacy-aware IoT-forensics," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Sydney, NSW, Australia, Aug. 2017, pp. 626–633.

Jianwei Hou received the B.S. degree in information security from Harbin Engineering University, Harbin, China, in 2016. She is currently pursuing the Ph.D. degree with the School of Information, Renmin University of China, Beijing, China.

Her current research interests include software-defined networking, Internet of Things, security, and digital forensics.

Yuewei Li received the B.S. degree in information security from the University of Science and Technology Beijing, Beijing, China. He is currently pursuing the M.S. degree with the School of Information, Renmin University of China, Beijing.

His current research interests include cloud security, trusted computing, and Internet of Things security.

Jingyang Yu received the B.S. degree in computer science and technology from Shandong University, Jinan, China, and the M.S. degree in applied mathematics from Henan University, Kaifeng, China. She is currently pursuing the Ph.D. degree with the School of Information, Renmin University of China, Beijing, China.

Her current research interests include searchable encryption, data security and privacy, and data security of Internet of Things.

Wenchang Shi received the B.S. degree in computer science from the Department of Computer Science and Technology, Peking University, Beijing, China, and the Ph.D. degree in computer science from the Institute of Software, Chinese Academy of Sciences, Beijing.

He is currently a Professor with the School of Information, Renmin University of China, Beijing. His current research interests include system security, trusted computing, and digital forensics.

Prof. Shi is the Vice President of the China Cyber and Information Law Society, the Vice Chair of the Academic Committee, China Cloud Security Alliance, and a Steering Committee Member of Cybersecurity Education, Ministry of Education, China.