A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues

Maria Stoyanova, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis

***Abstract*—Today is the era of the Internet of Things (IoT). The recent advances in hardware and information technology have accelerated the deployment of billions of interconnected, smart and adaptive devices in critical infrastructures like health, transportation, environmental control, and home automation. Transferring data over a network without requiring any kind of human-to-computer or human-to-human interaction, brings reliability and convenience to consumers, but also opens a new world of opportunity for intruders, and introduces a whole set of unique and complicated questions to the field of Digital Forensics. Although IoT data could be a rich source of evidence, forensics professionals cope with diverse problems, starting from the huge variety of IoT devices and non-standard formats, to the multi-tenant cloud infrastructure and the resulting multi-jurisdictional litigations. A further challenge is the end-to-end encryption which represents a trade-off between users' right to privacy and the success of the forensics investigation. Due to its volatile nature, digital evidence has to be acquired and analyzed using validated tools and techniques that ensure the maintenance of the Chain of Custody. Therefore, the purpose of this paper is to identify and discuss the main issues involved in the complex process of IoT-based investigations, particularly all legal, privacy and cloud security challenges. Furthermore, this work provides an overview of the past and current theoretical models in the digital forensics science. Special attention is paid to frameworks that aim to extract data in a privacy-preserving manner or secure the evidence integrity using decentralized blockchain-based solutions. In addition, the present paper addresses the ongoing Forensics-as-a-Service (FaaS) paradigm, as well as some promising cross-cutting data reduction and forensics intelligence techniques. Finally, several other research trends and open issues are presented, with emphasis on the need for proactive Forensics Readiness strategies and generally agreed-upon standards.**

***Index Terms*—Internet of Things, IoT forensics challenges, cloud forensics, security and privacy challenges, smart city forensics, IoV forensics, wearable device forensics, smart home forensics, digital forensics approaches, blockchain forensics, privacy-aware forensics.**

Manuscript received March 26, 2019; revised October 13, 2019; accepted December 15, 2019. Date of publication January 6, 2020; date of current version May 28, 2020. This work was supported by SPHINX project through the European Union's Horizon 2020 Research and Innovation Programme (Digital Society, Trust & Cyber Security E-Health, Well-Being and Ageing) under Grant 826183. *(Corresponding author: Yannis Nikoloudakis.)*

Maria Stoyanova is with the Faculty of Mathematics and Natural Sciences, Institute of Physics, Technical University of Berlin, 10623 Berlin, Germany.

Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis are with the Department of Electrical and Computer Engineering, Hellenic Mediterranean University, 71410 Heraklion, Greece (e-mail: nikoloudakis@pasiphae.eu).

Digital Object Identifier 10.1109/COMST.2019.2962586

I. Introduction

THE Internet of Things (IoT) is a well-known paradigm that defines a dynamic environment of interrelated computing devices with different components for seamless connectivity and data transfer. Technologies that are often implemented in the IoT domain are machine-to-machine communication (M2M), context-aware computing and radio-frequency identification (RFID). Some typical examples of such proactively sensing and adapting objects include: i) wearable devices like smartwatches, glasses or health monitoring systems, ii) smart home appliances like smart locks, sensors for temperature, gas or ambient light, iii) smart vehicles, drones and applications for industrial automation and logistics.

IoT devices exchange data with millions of other devices around the globe. Such type of open large-scale communication makes them especially inviting for users with illegal intentions. Only in 2017 there was 600 percent increase in attacks against IoT devices [1]. In many cases, the intruders are not directly targeting the IoT device, but using it as a weapon to attack other websites [2]. As a result, cybercrime has become the second most reported crime globally [3].

IoT systems seem to be easy targets for attackers, mostly due to the fact that when building an IoT device, manufacturers often place great emphasis on cost, size and usability, while security and forensics aspects tend to be neglected. Lally and Sgandurra [4] outline that some producers implement security practices mainly because an eventual exploitation of one of their IoT products will damage the company's image [4].

A. The Aim of This Paper

Even though the emerging technological advances like low cost image/video capturing and information processing techniques such as artificial intelligence and machine learning, have improved the forensic analysis level, there are still some significant challenges ahead. Therefore, the main goal of this paper is to take a closer look at vulnerability issues within IoT systems from a forensic point of view and examine the state-of-art Digital Forensics approaches.

More precisely, this work presents a compact survey of the fundamental challenges, theoretical frameworks and research trends in the IoT Forensics. Furthermore, it highlights the need for standardizing the forensics process, as it argues that this is a critical step towards high quality cross-jurisdictional forensics reports and cyber-security best practices. Another equally

important goal of this paper is to discuss the highly challenging issues of accessing personal data in a privacy-preserving manner (see Chapter Privacy-aware IoT Forensics).

Taken as a whole, this survey aims to answer the following questions: i) Which are the novel factors affecting the well-known digital forensics discipline? ii) Can the data stemming from IoT devices be utilized for forensic purposes, and if so, how useful can it be in the forensic investigation process? iii) Are there any techniques and models that collect, preserve and analyze data in an efficient forensic manner? iv) Are there any standards, regulations and best practice guidelines that could provide assistance to the digital forensics professionals? v) What are the current trends and open issues in the IoT Forensics?

B. Related Work

Since the introduction of cloud and fog computing, extensive research [5]–[8] has been conducted on cloud-based security issues. However, security and forensics are considered different disciplines, even though they share the same concerns. In contrast to security experts, whose goal is to minimize the risk of potential threats or the consequences of an occurring attack, the forensics professionals investigate the damage and the origin of the attack post-mortem. Hence, both disciplines use different tools and techniques (see Table I). And yet, similar to some prior work [9] that sees forensics and security as converging subjects, this survey also acknowledges the overlap between both fields by stating that digital forensics policies could be also considered security best practices.

Being forensically ready enhances the security level in both cloud and traditional computing. Therefore, some works found in cloud and network security such as [10], [11], could also apply to IoT-centered forensics investigations. After all, IoT networks impose the same vulnerabilities as long-established computer networks do. However, IoT systems interact with the physical environment more frequently, and therefore attract more threats, both physical and digital. For that reason, another huge part of the research is focused on the issue of securing the IoT domain [12]–[15].

In general, nearly every aspect in the IoT has been examined in extensive literature reviews [16]–[19], starting from the key enabling technologies and architectural elements, to fields of deployment and open challenges. Accordingly, there are also a vast number of papers [20]–[24], that deal with the wireless networks used in IoT communications. For example, scholars such as [25]–[28], discuss how the forthcoming 5G will look like and how it will reshape the future of wireless communication.

Although so many studies are conducted on cellular networks, cloud, and even IoT security, the literature on IoT Forensics is rather scarce. There are only a few surveys that examine the current IoT Forensics challenges and approaches, such as the work of Conti *et al.* [29], MacDermott *et al.* [30], Alenezi [31], Lilis *et al.* [32], Arafat *et al.* [33], and Zawoad and Hasan [34]. However, none of these papers offers the comprehensiveness of the present work.

In one of the most recent surveys, Yaqoob *et al.* [35] give an overview of the IoT-related forensic advances and open challenges. Their approach is similar to the assessment of this paper, with the exception that they are focusing on taxonomy and requirements, while this survey pays special attention to past and current frameworks, as well as to standardization and certification issues within the IoT Forensics discipline.

With regards to the existing digital forensics tools and approaches, the literature suggests two different paths. Some authors like [36], [37], propose holistic frameworks that are supposed to apply to the broader forensic context. Other scholars criticize this approach as too generic and choose to focus on specific use cases like a forensic framework for the Amazon Alexa ecosystem [38] or the Apple Smartwatch [39].

Prior research has examined, for example, specialized IoT networks such as industrial systems [40], [41]. Furthermore, a large number of works has looked at security vulnerabilities in personal IoT devices and smart home environments, including IP cameras [42] and smart locks [43]. The community has also largely discussed cyber-attacks against rather traditional IoT networks such as smart grids [44]. In addition, several surveys were previously conducted on autonomous vehicles and smart transportation systems [45]–[48], or drones [49]–[52].

Nevertheless, only a few works dive deeper in the description of standards and guidelines for acquisition and analysis of digital evidence. Some researchers such as Karie *et al.* [53] propose recommendations on how to handle a digital forensics investigation in a forensically sound manner, however, they do not explicitly focus on IoT-based incidents.

In general, the research done so far describes the present state of the IoT networks and does not attempt to hypothesize on near-future systems. Furthermore, none of the earlier mentioned works addresses issues such as forensic-specialized information retrieval techniques or forensics education for first responders. In addition, topics like suitability and usability aspects of forensic tools have not been covered sufficiently. The goal of this survey paper, therefore, is to summarize previous publications and complement them with up-to-date knowledge on the IoT-related forensics topics that have been so far rather neglected by the contemporary literature.

C. The Structure of the Paper

The structure of this paper is defined as follows: Section I is introductory. Section II deals with the necessary terminology specifications and clarifies the need for a separate discipline that operates in the IoT context. It further motivates this work by introducing the current and oncoming IoT market tendencies, as well as the industrial branches where IoT Forensics is expected to have a huge future impact.

Section III presents the current IoT Forensics challenges by dividing them into the following main categories: identification, acquisition, evidence analysis and correlation, attack/deficit attribution, and finally, presentation.

Section IV provides a review of the IoT Forensics approaches and their complexity. Special attention is paid to the most popular digital forensics techniques, e.g., the application of the 1-2-3-Zones Approach [54], as well as to

some other, more recent, IoT-centered frameworks that aim to extract evidence data without violating users' right of privacy [55], [56], or use blockchain to decentralize the forensics investigation process [57], [58]. This section also presents the most important aspects and frameworks in the mobility forensics field.

Section V deals with the indispensable open issues in the IoT Forensics. Besides present-day standards and best practice guidelines, this section refers to concepts like Digital Forensics-as-a-Service (DFaaS) and Error Mitigation Analysis.

Finally, in Section VI, this survey concludes with a reflexion on the presented findings. Besides discussing some promising solutions, this chapter aims at picturing the digital forensics discipline in the days of Internet of Everything.

In order to assist the readers, a list of used acronyms is provided in the Appendix of this work.

II. Definitions and Taxonomies

A. What Is Digital Forensics?

The discipline of Digital Forensics (DF) is a branch of the traditional forensics science. It concerns the uncovering and interpretation of electronic data. DF professionals deal with the identification, collection, recovery, analysis, and preservation of digital evidence, found on various types of electronic devices [59]. Consecutively executed, all above-mentioned steps constitute the Forensics Investigation Life Cycle [60], [61]. Although there are some variations in the way different scholars divide the investigation cycle into phases, one important detail should never be missed: the whole cycle should be executed using validated tools and scientifically proven methodology [62]. Since nowadays there are new platforms based on embedded technologies, DF investigators develop and validate new tools in order to keep pace with the advances, and guarantee the accurate and timely data extraction [63].

B. What Is IoT Forensics and How Is It Different From the Digital Forensics?

The IoT Forensics could be perceived as a subdivision of the Digital Forensics. However, while the DF discipline has long been in both academia and industry, IoT Forensics is a relatively new and unexplored area. The purpose of the IoT Forensics is similar to the one of the Digital Forensics, which is to identify and extract digital information in a legal and forensically sound manner. Besides from a particular IoT device or sensor, forensic data could be gathered from the internal network (e.g., a firewall or a router) or from the cloud [2]. Following this, IoT Forensics could be divided into three categories: IoT device level, network forensics and cloud forensics (see Figure 1).

A fundamental difference between Digital Forensics and IoT Forensics could be seen in terms of evidence source. Unlike traditional DF, where the usual objects of examination are computers, smartphones, tablets, servers or gateways, in IoT Forensics the sources of evidence could be much more wide-ranging, including infant or patient monitoring systems, In-Vehicle Infotainment (IVI) systems, traffic lights, and even medical implants in humans and animals.

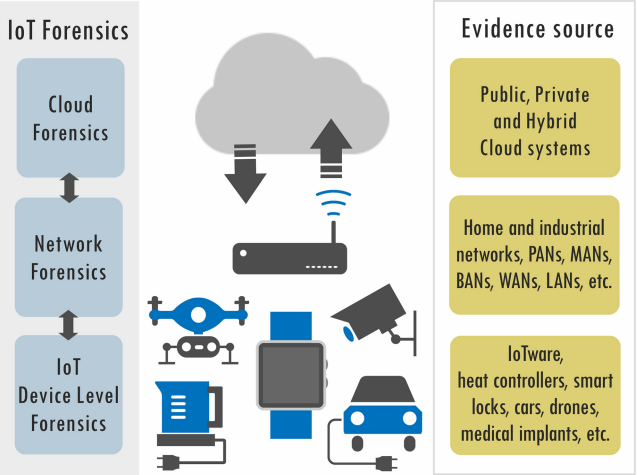

Fig. 1. Components of the IoT Forensics.

C. How Are IoT Forensics and IoT Security Different?

To secure every single sensor, communication device and cloud storage within the IoT network, is nearly impossible. If an incident happens, one of the first tasks that forensics professionals execute is to define the scope of the compromise. However, unlike IoT security practices, forensics techniques do not aim to minimize the damage, but to identify the attack/deficit origin or the liabilities of the different parties. The further differences between the two disciplines are summarized in Table I.

D. Why Do We Need IoT Forensics?

Argument 1 (Extensive Attack Surface): Machine-to-machine (M2M) technology has expanded rapidly in the recent years, but despite all the benefits and wide prospects of this advanced idea, M2M is an example of particularly vulnerable to cyber-attacks type of communication. It is associated with a large number of terminals and a large amount of embedded hardware (like location tags and smart sensors) which increases its attack surface and puts it at higher risk [41]. The same applies to IoT which evolved on the foundations laid down by M2M technology.

Accordingly, IoT devices with public interfaces are exposed to greater risk levels because they could bring a malware to the private network from a less secure public space [65]. Commonly seen incidents include identity theft and data leakage, accessing and using Internet connected printers, node tampering, commandeering of cloud-based CCTV units, SQL injections, phishing, insurance related fraud, cyberbullying, ransomware and malware targeting specific appliances such as VoIP devices and smart vehicles.

Cyber-attacks could also have a large-scale nature and affect global enterprises or create chaos in the stock market [66]. For example, IoT devices can be used to launch Distributed Denial of Service (DDoS) attacks against third-party websites, corporate networks or governmental institutions [40]. The second largest DDoS attack so far took place in October 2016 and was directed at Dyn, a well-established DNS provider. By using a malware called Mirai, the attackers created a botnet

TABLE I
FUNDAMENTAL DIFFERENCES BETWEEN IOT SECURITY AND IOT FORENSICS [64]

IoT Security	*IoT Forensics*
Provides security insurance for both physical and logical security issues	Determines and reconstructs the chain of events by analyzing physical evidence and electronic data
Applies diverse security techniques to minimize the scope of the attack and prevent further damage	Applies investigative techniques to identify, extract, preserve, and analyze digital information
Real-time response: implements different techniques in order to confront the threats during a live incident	Post-mortem investigation: identifies deficits after the incident occurred or while the system is inactive (however, when applying live forensics techniques, forensics professionals acquire digital evidence during a real-time incident)
Generalized: looking for any possible harmful behavior	Case-centered: reconstructing a given criminal scenario
Continuous process: keeps alert 24 hours a day	Time-restricted process: after a crime is alleged to have occurred (notitia criminis)
Security training and awareness: applies a set of security procedures, processes and standards, in order to have a securely-ready system, and prevent future cyber-threats from happening	Forensics Readiness: meets the forensics requirements and applies forensics standards, in order to be ready to undertake an investigation; takes measurements to maximize the forensic value of the potential evidence, and minimize the amount of resources spent on the investigation
Specifies the judicial region and legal aspects in service legal agreements regarding the security	Specify the judicial region and legal aspects in service legal agreements regarding the forensics issues
Well-established computer science field	Young and unexplored branch of the Digital Forensics

out of compromised IoT devices such as smart TVs, IP cameras, printers, etc. [67]. As a result, there were irregularities for many sites, including platforms like Amazon, Twitter, PayPal, Visa, AirBnB, Netflix, Spotify, Tumblr, The New York Times, Reddit, and GitHub. Gartner have estimated that by 2020, more than one quarter of the attacks will involve compromised disparate devices [68].

Argument 2 (New Cyber-Physical Security Threats): Furthermore, Alabdulsalam *et al.* [2] state that by using the power of IoT technology, virtual crimes could step across the limit of cyberspace and threaten human life. The authors bring to notice a case from January 2017, when the U.S. Food and Drug Administration (FDA) published a warning that certain pacemaker models (a device used by patients with heart arrhythmia to regulate the heart muscle contractions) were vulnerable to hacking [69]. Another vulnerability was detected in the portal login process of an LG smart vacuum cleaner, allowing a group of researchers to access live video stream from inside the owner's home [2]. In a similar incident, CCTV units for infant monitoring (commonly referred to as "nanny cams") have been accessed and the footage made available to the public.

Smart locks, for instance, could be programmed to unlock if a particular device is detected by the wireless network of the building, allowing a criminal to access someone's home or office. A scenario with lethal consequences would be plausible if a smart lock is programmed to lock when a fire or gas leak is detected [65]. Such a situation could be both the result of an intentional attack or consequence of a malfunction due to an inadequate design and a lack of system adaptation.

Thus, while the attack types [70], [71], illustrated in Figure 2 have already been experienced, IoT introduces new cyber-physical threats to users and forensics investigators. In other words, IoT could transform some of the existing digital risks by turning them from privacy and digital security threats to physical security threats.

Argument 3 (Digital Traces): Servida and Casey [72] use the term digital traces to describe a piece of information (stored on smartphones and IoT devices) which is able to prove or disprove certain hypothesis, and could therefore help the forensics professionals find answers and reconstruct the crime scene [68]. For example, digital traces may give information about when a smart home alarm was disabled and a certain door was opened. Also, the information gathered from a smoke or carbon monoxide detector could determine the exact moment and place where the fire in the building started [72]. Wearable devices like smartwatches or fitness trackers can be used to identify a person via their biometric information (e.g., heart-rate) [68].

According to [73], examples for such forensic artefacts may include cached image thumbnails and fragments of the camera streams, as well as cached events triggered by the sensors, and complete event logs stored in the application database. Certainly, these files include sensitive personal information about users' identity, location, activity, as well as general linkages and chronology, and therefore must be gathered and analyzed with special attention to ethics and privacy (see Section Privacy and ethical considerations by accessing personal data).

E. Where Do We Need the IoT Forensics the Most?

The IoT market has and will continue to experience an exponential growth over the current decade as shown in Figure 3. Starting from 157 billion USD in 2016, the IoT market value has been projected to reach a market cap extending to 771 billion USD by 2026 [74], [75]. Cisco predicted that by the year 2030, 500 billion objects will be connected and linked up to the Internet [76].

Cloud service providers have seen this as an opportunity to establish new business models. Thereby, the

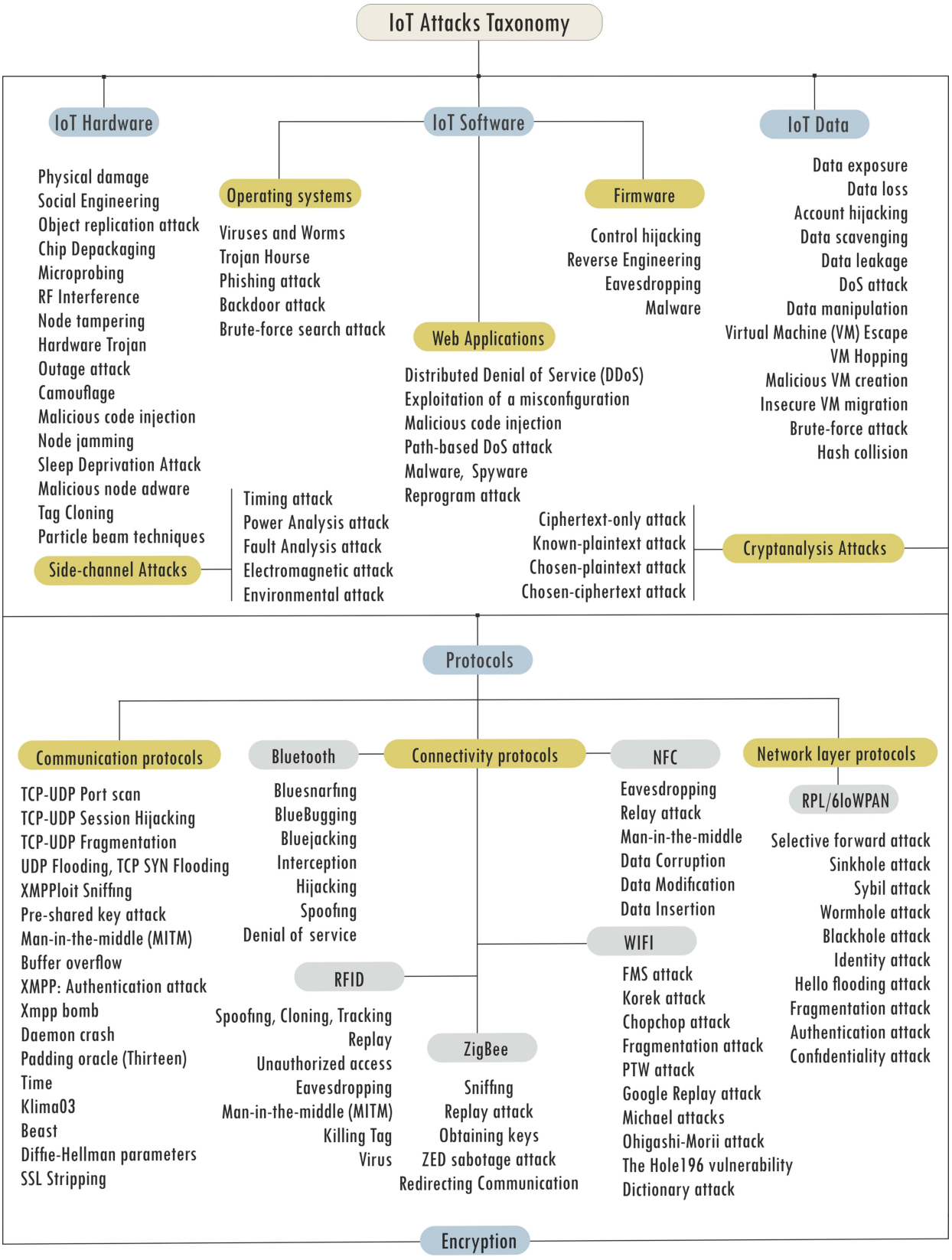

Fig. 2. Classification of the IoT Attacks [70], [71].

ongoing Forensics-as-a-Service (FaaS) paradigm has started (see Section Forensics-by-Design). Securing the whole IoT network, however, is not an easy task. Unlike conventional computing devices which rely on traditional network security suites like endpoint protection and firewalls, IoT communication consists of endless number of protocols,

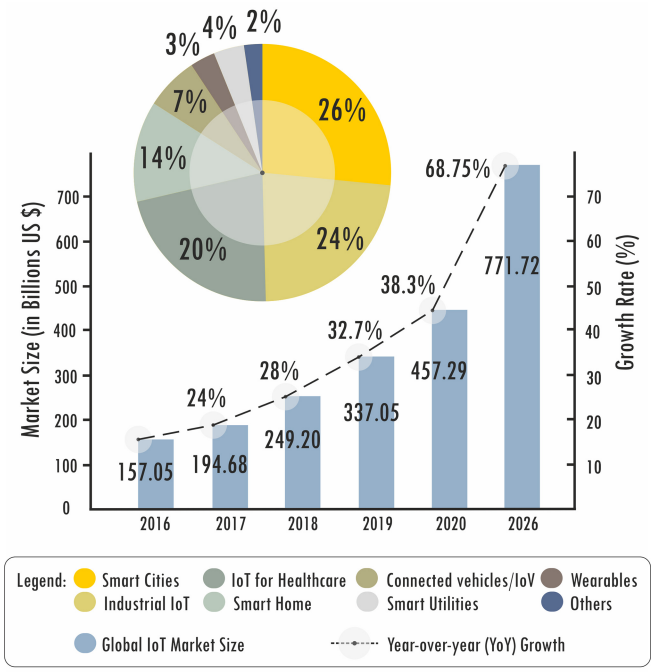

Fig. 3. Global IoT Market size (2016 - 2026), according to [74], [75].

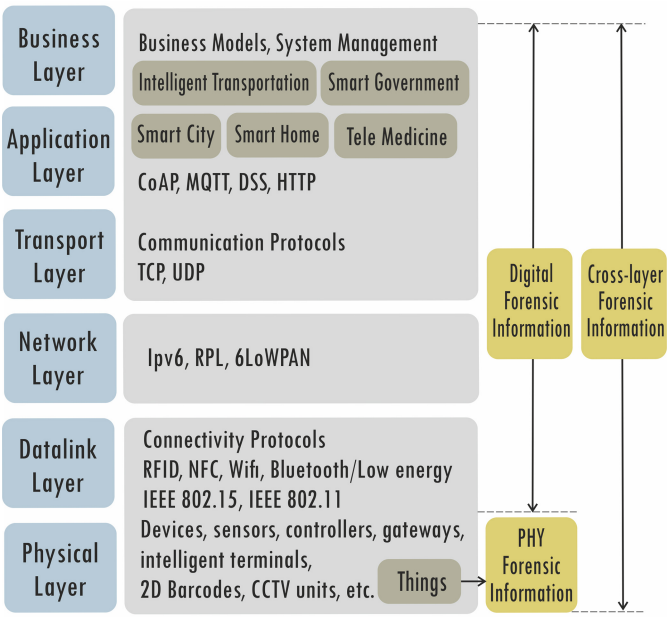

Fig. 4. IoT-layered Architecture [40], [64], [70].

device capabilities and standards. Thus, IoT security relies upon securing each and every layer shown on Figure 4.

Accordingly, the IoT security and forensics tools are in high demand [77]. This applies to all IoT-based domains like healthcare, smart home appliances, industrial machines, supply chain and inventory management, smart grid, surveillance, and smart cities. Industries, which rely on sensitive data for real-time decision making, are among the most appealing ones for the attackers. Hence, this is where forensics expertise will be most needed in the next couple of years.

1) IoT Forensics for Smart City and Vehicle Automation: Smart Cities are cyber-physical ecosystems that optimize the usage of the conventional city infrastructures such as road and railway networks, parking spaces, power grids, oil and gas pipelines, water systems, etc. By doing so, Smart Cities offer novel and convenient (digital) services to their citizens [78]. Smart parking for example, is an ongoing topic not only in academia, but also among metropolitan city governments and auto-tech companies. A comprehensive study by Al-Turjman and Malekloo [79] shows the current state-of-the-art in this field by presenting a classification of the major smart parking technologies, sensors, design factors, and solutions for smart ecosystems or single vehicle-detection.

The authors additionally acknowledge another current trend in the developing IoT domain, namely the Unmanned Aerial Vehicles (UAVs). Colloquially known as drones, UAVs have captivated the public interest. Some of the leading logistics firms such as DHL, Amazon, and UPS, launched new UAV-based delivery services. By using drone technology, these logistics companies hope to revolutionize the first and last mile delivery in mega cities and rural areas. Since the recent advances made model drones (essentially non-commercial devices) easily affordable, sales and registrations are continuously increasing. According to a recent five-year forecast [80], the global drone market is expected to reach a value of $43 billion by the end of 2024.

Among other critical applications, UAVs are used to perform tasks where time and cost should be reduced to a minimum. In case of extreme situations, for example after a hurricane disaster, Al-Turjman *et al.* [49] suggest using drones to setup base stations and provide cellular coverage over the given area in danger. Same technique could be also applied for densely populated urban areas (e.g., stadiums), in order to maximize the 5G coverage in a relatively inexpensive way (for further details on UAVs forensics see Chapter Mobility Forensics Frameworks).

Undoubtedly, one of the trademarks of the smart city is its intelligent transportation systems, more precisely the so-called Autonomous Automated Vehicles (AAVs). Equipped with sensors for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, smart cars and buses can provide the necessary information to passengers, drivers, or agencies for efficient and safe city traffic [78]. Some of the contemporary automobile manufacturers such as Tesla, BMW, Mercedes and Daimler, have already released vehicles with self-driving features. Tech companies like Google and Uber have also demonstrated autonomous driving prototypes on real roads [81]. According to the business information provider IHS Markit [82], by 2035, there will be almost 11.8 million connected vehicles that offer automated-driving assistance and other modern in-vehicle services [46].

The fast IoV development and implementation will bring some new challenges, especially in terms of security. Various attackers have already tried to exploit AAVs' communication channels and trigger malicious instructions that affect the braking and engine system [83]. For example, a smart vehicle could be compromised during an operating system update, and exploited to alter sensor data that is sent to other vehicles via the V2V and V2I interface [47]. The same way,

a malicious smartphone app could attack a smart vehicle or a roadsite unit (RSU) via the vehicle-to-consumer electronics (V2CE) interface [47]. In addition, compromised AAVs could be used to create a botnet und initiate large DDoS attacks like the one presented in the previous section (see Argument 1 in Section: Why do we need IoT Forensics?).

Especially interesting from a forensics point of view is the Vehicle Infotainment system because it stores a vast amount of user-related data (e.g., the navigation history of the vehicle, call logs and contact lists, pictures, videos, etc.) [84]. Forensics professionals could use such information to identify liabilities in traffic accidents or cyber-attacks. Moreover, in case of an accident, they could examine the sensor records from the neighbouring cars. Since build-in proactive urban monitoring solutions like MobEyes [81] or Pics-on-Wheels [85] record the surroundings while driving, forensics professionals could even search the vehicular network for video material of the accident. Of course, the massive deployment of sensors and the huge amount of IoV data brings the traditional forensics practices into challenge and demands new, intelligent forensic techniques for autonomous vehicles (see Section Mobility Forensics Frameworks).

2) IoT Forensics for Smart Home/Office: Smart Building applications support personalization by controlling over the living and working environment. A system formed by sensors and actuators aims to enhance the comfort of the residents, usually even without their intervention. Moreover, by enabling owners or managers to monitor the property remotely, smart home systems contribute to the building's maintenance and safety. Air conditioners, floor heating systems, refrigerators, washing machines, and lights could be controlled over the Internet in order to save energy, water and other resources. Besides sustainability and efficiency, smart building solutions could also offer assistance during emergency situations. For example, fire alarms could be automatically activated, based on the readings of the temperature sensors and smoke detectors [76].

By 2023, the smart home market is expected to reach $141.2 billion, which will mean a 17% increase compared to 2019 [86]. However, while smart home and office features bring well-understood benefits to our daily lives and increase our comfort, they also imply wide attacking surfaces, and thus raise critical concerns in the notion of trust, privacy, and security.

Some Internet-connected home appliances, for example, are programmed to perform a self-check and request a repair service in case of a technical problem. If there is a need for repairs, the intelligent building system could ensure the technician's access to the broken device. Criminals might be attracted to this feature and manipulate the system in order to enter the home while the residents are away [65]. In the context of a smart factory, intelligent features may create new opportunities for ad-hoc attacks like industrial espionage and cyber-sabotage [66].

Finally, as already illustrated (see Argument 2 in Section: Why do we need IoT Forensics?), smart home systems may introduce some new cyber-physical threats. Sensors for emergency detection (e.g., gas leak identifier) are supposed to automatically notify an external emergency service, and open all doors and windows in the building. However, a rogue device impersonating these sensors may be used to let an intruder in, or even worse: block the notification of the emergency unit and lock the exits [65].

3) IoT Forensics for Healthcare: Among all IoT-based domains, the healthcare sector is probably the most vulnerable to major security attacks. This could be explained with the cross-organizational nature of IoT applications in this field, as well as with their heterogeneity, fragmentation and expanded attack surface [76]. So while transforming the healthcare industry and improving human life, remote health monitoring devices evoke some new concerns about protection and security of users' medical data [76].

Fitness trackers, for example, could be targeted by malicious actors who want to use the gathered data for illicit financial gains, e.g., by selling it to insurance companies or blackmailing the owner of the compromised device [65]. The increasing number of medical identity theft cases is not surprising, given the high value of medical data. In general, the market size of mHealth applications and services was valued over $86.4 billion in 2018, and is expected to witness more than 29.6% compound annual growth from 2019 to 2025 [87].

Wearables like fitness bracelets have also gained importance in the forensics for another reason, namely as a source of digital evidence. They are programmed to work passively in the background of users' daily life and generate data with build-in sensors (e.g., measuring distance walked, heartbeat, body temperature, calorie consumption, sleep-wake rhythm, etc.). Therefore, they could provide a large amount of forensic data that could be utilized to refute the false testimony of a suspect or to trace the activities of the victim, near the time of the incident. Thus, originally designed to monitor a user's health status, the IoT-based applications could also play the role of the so-called "digital witness" [65]. For that reason, the study of smartwatches and fitness band trackers has become even more attractive to the forensics practice.

Another reason is the increasing popularity of these devices. According to Gartner, Inc. [88], the global wearable technology sales for 2019 will reach 225 million. Smartwatches are the current top wearables segment with 74 million shipments [88]. Nevertheless, until the present moment there are very few studies conducted on the topic of how smartwatches or other wearable devices could be used as source of digital evidence. By researching this subject, there should be special attention paid to the privacy-related issues, since the data gathered could be extremely sensitive.

The increasing number of security and privacy incidents only highlights the need for innovative, multi-faceted approaches, different and much more powerful than the established digital forensics methodology [63]. The following Chapter will further illustrate the challenges in the forensics landscape, as well as the complexity, dynamicity and high connectivity of IoT-enabled ecosystems.

III. Current Forensic Challenges Within the IoT

The IoT Forensics field is encountering an array of challenges, none of which has a simple solution [89].

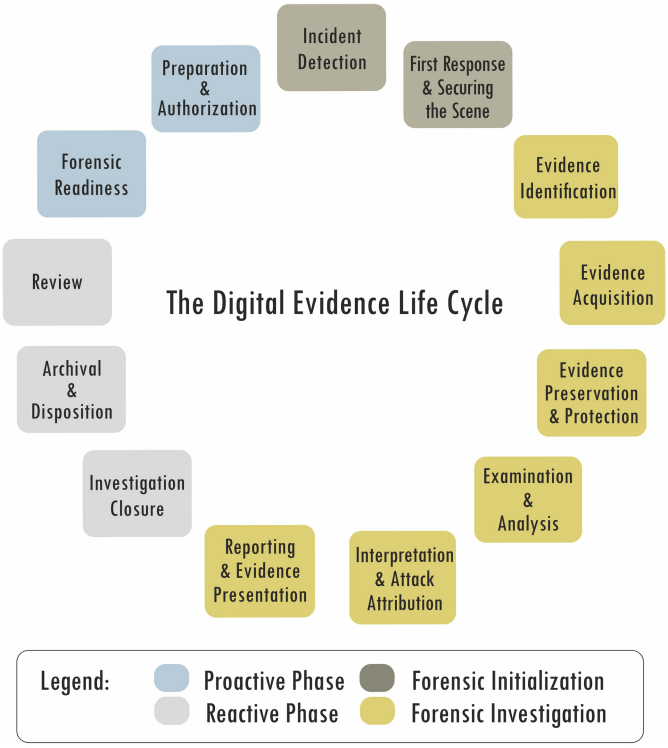

Fig. 5. The Forensics Evidence Life Cycle.

A comprehensive list [90] provided by the U.S. National Institute of Standards and Technology (NIST) identifies 65 challenges associated with cloud and IoT Forensics. The NIST scientists divided all problematic issues into seven categories, the most prominent of which is the multi-tenant nature of the cloud, followed by the complicated evidence acquisition procedure [91]. Al-Fahdi *et al.* [92] conducted another survey among forensic practitioners and researchers and found out that both groups place time and vast data volume on top three of the most challenging issues. However, according to forensics practitioners, legal aspects represent another significant challenge, while researchers believe that automation in forensics is the third most important topic [93].

Following [29], [94], this work divides the most challenging forensics aspects into six groups: identification, collection, preservation, analysis and correlation, attack attribution, and finally, evidence presentation (see Figure 5).

A. Evidence Identification

The first and probably the most essential part of any forensic examination is the search for evidence [29]. Hegarty *et al.* [95] assert that identification in the IoT context is especially difficult, since in some cases the examiners do not even know where the investigated data is physically stored [96]. Even a simple task like finding the compromised IoT device and reconstructing the crime scene could be challenging. The following lines explain what problems the investigators encounter during this very first step of the Forensics Investigation Life Cycle.

1) Scope of the Compromise and Crime Scene Reconstruction: In traditional (digital) forensics, boundary lines could be easily defined: investigators could determine the number of devices that have to be confiscated, or the number of people that were using a compromised device [54]. The IoT context, however, implies real-time and autonomous interaction between various nodes, which makes it almost impossible to reconstruct the crime scene and to identify the scope of the damage [29], due to the highly dynamic nature of the communication. The data could be stored on different virtual machines (VMs), which means that important forensic data such as registry entries or temporary files could be completely erased as soon as the VM gets rebooted or turned off [97].

2) Device and Data Proliferation: The increasing number of interconnected devices and the amount of digital forensic data requiring analysis, has been discussed over many years [98]. A report conducted by the International Data Corporation (IDC) states that the estimated growth of data from 2005 to 2020 is expected to be 40.000 exabytes [96]. Hence, the traditional digital forensics tools are incapable of handling such tremendous increase in volume, variety and velocity [34]. Forensics professionals not only have to identify what is useful for the investigation, but also to discard the irrelevant data, which makes the timely analysis difficult [68].

3) Data Location: While operating, IoT devices could frequently migrate between different physical locations. For example, when people travel, carrying their personal electronic equipment with them, Body Area Networks (BANs) move between different Wide Area Networks (WANs) [54]. Data descending from fitness trackers, smartwatches, smart clothing, or larger movable objects such as cars, bikes and drones, is not fixed in a particular geographic place. Instead of being confined to a single host or data centre, it is rather dispersed among different cloud recourses, personal network-attached storage units, crypto-currency wallets, online social networks, etc. [66].

Therefore, when attempting to locate evidence, digital forensics professionals face considerable challenges. Even if the location is known, acquiring the system is not without any complications because it could affect other customers who are using the same architecture [33]. Moreover, the resources may be subject to multiple jurisdictions with numerous, and even contradictory regulations on data protection and unauthorized intrusions [2]. If the law in one country grants access to smart devices, criminals might hamper the investigation process by mailing their wearable device to another country or parking their smart vehicle behind the closest border [66].

4) Device Type: In contrast to the traditional digital forensics science, where the objects of forensic interest are usually limited to different types of computer systems or mobile phones, the source of evidence in IoT-centric cases could be heterogeneous: starting from an autonomous vehicle that caused a fatal accident, to a smart toaster that turned on during the night and initiated a fire in the household. Some IoT devices could be hard to find by the forensics professionals due to their small dimensions. Medical sensors, for example, the blood pressure measurement sensor by Merit Sensor Systems

Inc., could be only 8.1 x 10.5 mm big and weigh less than 2 grams [99]. Other IoT devices could be possibly hard to detect due to lack of battery life or because they could not be distinguished from traditional household appliances like refrigerators, dishwashers, pressing irons and baby monitors [100]. It is important to keep in mind that IoT devices are not designed to disturb our daily routines but to work passively in the background and engage only when needed [29].

B. Evidence Acquisition

Assuming that the relevant IoT device has been successfully identified, the second step would be to collect the evidence data. However, at this point the investigators must deal with another problem: until the present moment, there is no guidance or standardized method for evidence collection from an IoT device in a forensically sound manner [29].

The term "in a forensically sound manner" is extensively used in the Digital Forensics and implies that there must be a specific procedure applied while collecting the evidence information in order to make it usable in court [101]. For example, the process of evidence collection must begin in a lawful way, meaning that the corresponding authorities must issue a written order to initiate the investigation [61]. Furthermore, each step of the investigation process must be carefully documented in order to ensure a proper Chain of Custody (see Section: Securing the Chain of Custody).

In this regard, the evidence collection phase is one of the most crucial steps of the forensic procedure, because any error could make evidence material invalid and affect the whole investigation process [34]. A study of 100 random Digital Forensics lawsuits showed that in 8 out 100 cases, there was an error or contamination during the evidence collection step [91].

1) Lack of Training and Weak Knowledge Management: The NIST Forensics Science Challenges Report [90] identifies the need for cloud training for first responders and investigators. Rana *et al.* [89] also suggest that law enforcement agencies should organize training programs for their first responders in order to instruct them how to acquire digital evidence in a forensically sound manner. According to the authors, the responding officers often unplug or shut down the system directly, without first creating the necessary forensic image [89]. This makes evidence acquisition from IoT devices one of the most neglected steps in the practice. At the same time, by bridging the borders between decentralized on-scene units and research laboratories, the forensics practice could offer timely and legally appropriate digital and physical evidence analysis [73].

2) Data Encryption: Undoubtedly, encryption has always been one of the most challenging issues in Digital Forensics [32], [91], [102]. Nowadays, to improve consumer trust, many operating systems and platforms provide integrated support for encryption [91]. The algorithms allow users to encode the data before sending it to the cloud and decrypt it after returning to their own system.

The existence of such easy-to-use cryptographic tools has made it convenient for users to preserve the security of their data. Consequently, the percentage of the end-to-end encrypted files has increased [66].

However, by having full control over the cloud infrastructure, users could hide or manipulate information that cannot be recovered by the provider. The vendor must obtain the decryption key from the user in order to process the data and provide the investigating authorities with the necessary information. Hence, encryption represents a "trade-off" between the success of the investigation and citizen privacy rights [91]. Losavio *et al.* [103] concludes that maintaining that balance between the needs of the state and the needs of the citizens will play a central role in the future of the forensic discipline.

3) Heterogeneous Software and/or Hardware Specifications: Another technical challenge related to the extraction of evidence from IoT devices is that each manufacturer adopts different hardware and operating systems [32]. In addition to this complexity, communication protocols of IoT devices can be equally diverse, be it ZigBee, WiFi, Bluetooth, etc. [31].

Even if the evidence data could be retrieved from the IoT device, it may be stored in an encrypted way or in a non-standard format for which currently there is no applicable viewer. This means that in the first place, the files have to be decoded and converted to a readable form [54]. In overall, in order to be able to deal with any kind of IoT crime, the investigating unit has to possess knowledge about a huge amount of systems and standards.

4) Privacy and Ethical Considerations by Accessing Personal Data: Beyond technical challenges, privacy is a major issue to consider while collecting data. IoT devices such as fitness trackers or remote health monitoring systems, deal with sensitive personal information including users' medical records, prescriptions or current health status. In order to not violate confidentiality agreements with their customers, cloud service providers refuse to give authorities access to the shared memory, because it may also contain data of customers who are not related to the investigation [55], [104]. Especially in a multi-tenancy context, there are very limited methods to create a forensic image without violating any ethical considerations.

Most of the current forensics models have rather neglected the privacy aspect [35]. However, some considerable methodology towards privacy-aware IoT Forensics has been presented by Nieto *et al.* [55], [56]. Their work aims at adapting the so-called *digital witness solution* and making it compliant to the recently proposed PRoFIT model (see Section III). Other researchers from academia and industry concentrate on blockchain as a promising solution for many concerns in the IoT domain. The effectiveness of blockchain technology for security and privacy is demonstrated in [105]–[107].

Verma *et al.* [108] presented another privacy-preserving Digital Forensics framework. The authors propose to segregate the processed data into two separate categories, namely Forensically Relevant Files (FRF) and Forensically Irrelevant Files (FIF). Files labelled as irrelevant for the particular case will become inaccessible to the forensic examiners during the remaining investigation stages. Thus, this methodology

could ensure that the steps, following the evidence collection phase, will also be performed in a privacy-preserving manner. Although the presented approach has some limitations, it still offers an acceptable solution, especially for forensically non-related user files (for further information on approaches for privacy-preserving data acquisition see Section Privacy-aware IoT Forensics in Chapter III).

Similar to forensics practitioners and law enforcement agencies, companies also struggle when they have to manage forensically relevant data in a secure and privacy-preserving manner. A fundamental question in this context remains on how to assist the evidence collection process, and at the same time, guarantee users' right to privacy. In this regard, Dropbox has implemented a piece of software[1] for child abuse detection that allows searching within the stored material for breaches of the company's Terms of Use [109]. Nevertheless, scholars like Choo *et al.* [109] argue that in order to ensure the privacy of the individual, the investigation should rather focus on private suspect devices seized under a search warrant, than public surveillance like the case revealed in 2013 by the former NSA contractor Edward Snowden [109].

Since May 2018, the new General Data Privacy Regulation (GDPR) obligates organizations possessing data of EU residents, to take all necessary technical steps to ensure the security of the customers' Personally Identifiable Information (PII). For most of the firms, achieving GDPR compliance meant a huge amount of additional expenses. They had to hire a data controller, data processor and a data protection officer [110]. According to Forrester Research Inc. [111], large firms allocated on average $20 million to become GDPR-compliant, smaller ones around $5 million.

Back in 2018, many companies were under-prepared for the new regulation. Today, nearly two years after the new GDPR took effect, users and experts have still not reached a consensus on if and how the regulation has impacted data management practices. An overview of the implementation [112] by the European Data Protection Board (EDPB) announces a total of 206,326 data breach notifications and complains, as well as €56 million in fines (including the €50 million fine by the French data protection authority CNIL against Google on 21 January 2019 for improper possessing of personal information for advertising purposes). However, every forensics professional or lab researcher who is performing Digital Forensics and incident response in the European Union,[2] will have to know and apply the new regulations. The specific requirements that forensics practitioners have to take into account will be presented and discussed in Section V, Towards Standardization and Certification in IoT Forensics.

5) Forensic Value of Evidence: Some providers of IoT services stop supporting their frameworks and seize to deliver security updates. This applies especially to companies, part of the expanding start-up scene, which decide to concentrate on new products and stop supporting the old ones. Data gathered from such IoT devices is less valuable, because it could be easily manipulated by a hacker who took advantage of the security vulnerabilities. Apart from that, IoT data is often intermittent. Solar-powered nodes, for example, could contain only fragmentary information due to insufficient energy supply [66]. In general, data from IoT devices has limited forensics value since IoT devices could work without human interference and adjust to changes in the indoor/outdoor situation accordingly [96].

6) Lack of a Common Forensic Model in IoT: The theory and practice lack one commonly accepted and valid acquisition approach for IoT systems [29]. Depending on the case, the responsible investigative body chooses different methods. However, an unlucky choice of methodology could have many possible complications. On one hand, the evidence gathered can easily be challenged in court due to omissions in the way of collection [101]. On the other hand, cross-border crimes require co-operation between investigative bodies in two or more countries. Problems are encountered in the absence of supranational agreements. It is therefore necessary to unify the evidence-gathering approaches, because otherwise there is a risk to violate a local law, and consequently to render important evidence unreliable.

C. Evidence Preservation and Protection

In case investigators find one possibly compromised device and manage to collect potentially useful data, they will have to face another challenge: how to preserve the gathered data and guarantee its integrity.

1) Securing the Chain of Custody: The term "Chain of Custody" could be defined as the accurate auditing control of original evidence material [61]. In conventional forensics, it starts when the investigators gather a piece of evidence at the crime scene and ends with the presentation of the evidence material in court. As one of the fundamental issues in every forensic investigation, the purpose of the Chain of Custody is to provide clear information about when and how the evidence was gathered, preserved, analyzed and presented [97]. Moreover, it proves that the evidence material has not been altered or changed during all steps of the forensic investigation [58], [61], [113].

In the case of IoT Forensics, evidence data must be gathered from multiple remote servers, which significantly complicates the mission of maintaining proper Chain of Custody [104]. Additionally, the format of the data collected from a certain IoT device may be different from the format of data stored in the cloud. This is due to the fact that before being saved, it was processed by analytic algorithms [2]. Lastly, it has to be returned to its original format before executing the analysis, otherwise it will not be accepted in court.

Various scholars advocate the idea of a Digital Chain of Custody (DCoC). Some suggest using blockchain technology in order to protect the volatile nature of the digital

[1]Details of the software are not publically available.

[2]Same applies for forensics professionals in organizations doing business in the EU, or EU businesses that operate outside the EU market.

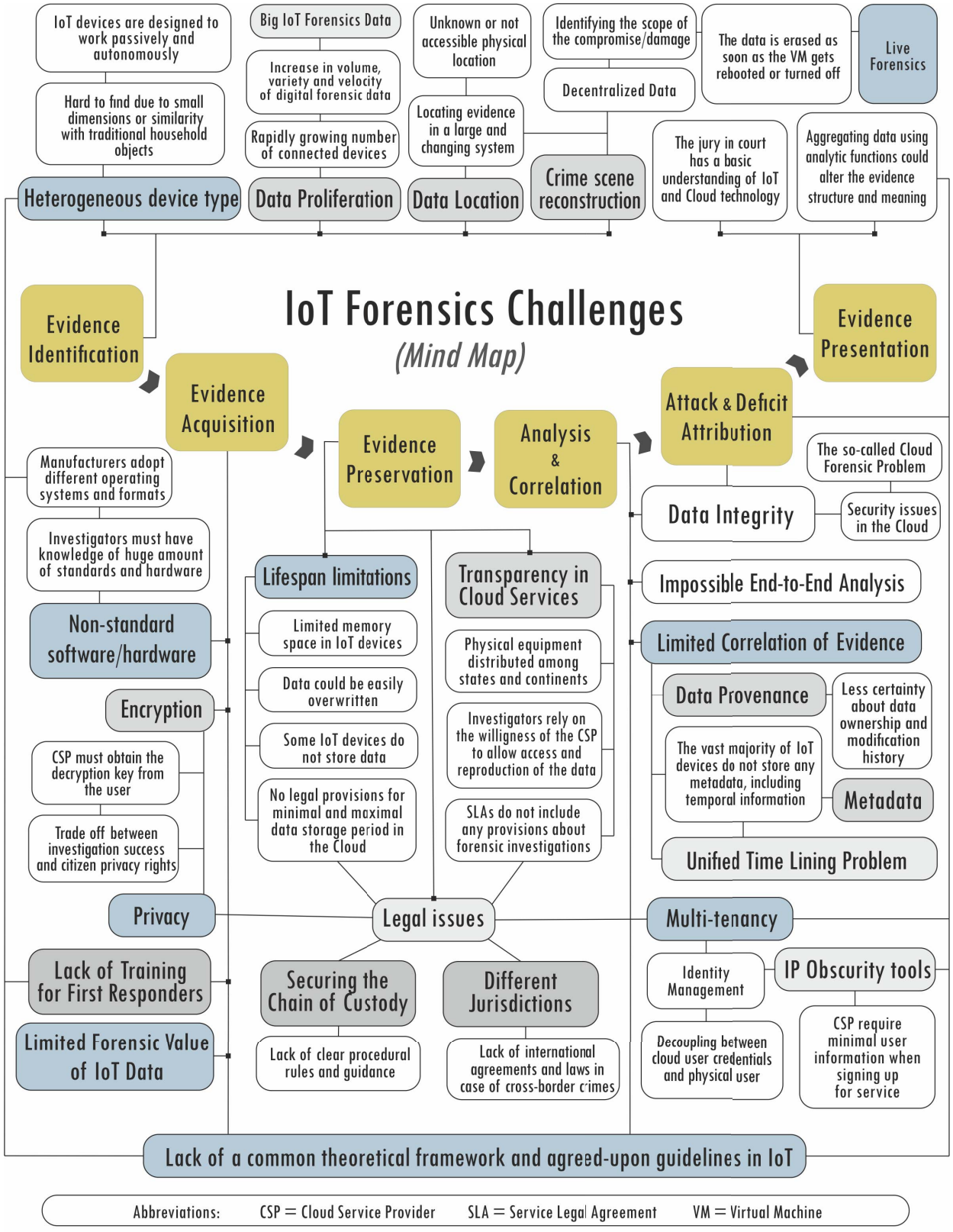

Fig. 6. Mind map of the IoT Forensics Challenges.

evidence in a highly decentralized environment. Others propose to go beyond the well-known DCoC concepts and use technical devices that take the role of a human witness. These so-called "digital witnesses" are supposed to manage electronic evidence from a both technological and legal perspective [114]. Securing the Digital Chain of Custody

through intermediary devices may offer some additional flexibility. However, there are also some limitations, for example regarding the format of the evidence information [114].

Due to its immaterial nature, digital evidence is especially vulnerable to manipulation, and therefore, it has to be extensively documented and protected during all steps of the forensic process. Figure 7 shows how, by using blockchain technology a certain piece of digital information can be preserved and routed towards its final destination, the court of law.

2) Lifespan Limitation: Another challenge in data preservation is related to the limited memory space in IoT devices. Due to the fact that IoT systems are running continuously, data could be easily overwritten, resulting in the possibility of missing evidence [35]. Transferring the data to a local storage device could seem like an easy solution in this case. However, this approach is unable to secure the abovementioned Chain of evidence, because data could be modified during the transfer [35]. In addition, some IoT devices employ Real-Time Operating Systems (RTOS) and do not store data by default [115].

3) The Cloud Forensic Problem(s): The synergy between cloud and IoT has emerged because the cloud possesses attributes which enable and benefit the IoT expansion [10]. However, the cloud consists of a huge amount of security issues. This is not surprising since cloud computing encompasses many technologies, including networks, virtualization, databases, operating systems, resource scheduling, load balancing, memory, and transaction management [116]. The vulnerabilities of all aforementioned systems reflect on the security in cloud architectural frameworks. Therefore, data preserved in the cloud has limited forensic value, since it could have been altered by a malicious user who took advantage of the vulnerabilities (see Section Forensic value of evidence).

A survey [117], conducted by the Cloud Security Alliance (CSA), identified the top twelve threats to cloud computing as follows:

1) Insecure APIs;
2) Account hijacking;
3) Weak identity, credential and access management;
4) System and application vulnerabilities;
5) Data breaches;
6) Malicious insiders;
7) Advanced Persistent Threats (APTs);
8) Insufficient Due Diligence;
9) Data loss;
10) Abuse and nefarious use of cloud services;
11) Denial of service;
12) Shared technology vulnerabilities.

Of course, no system is immune to attacks. However, cloud systems have one particular weakness that has not yet been resolved, namely the *"Cloud forensic problem"*. This fundamental challenge arises once the intruders gain access to the victim's system. From that moment on, they can modify and delete whatever data they want, including completely erasing all traces of the attack [110].

At the same time, it should be taken into account that the distributed nature of the cloud may also be an advantage for the forensics practice. Because of the way data is being managed in the cloud, traces left by criminals are harder to destroy. Digital evidence is usually mirrored in multiple places, or already hashed and indexed, which makes the collection of artefacts possible [66].

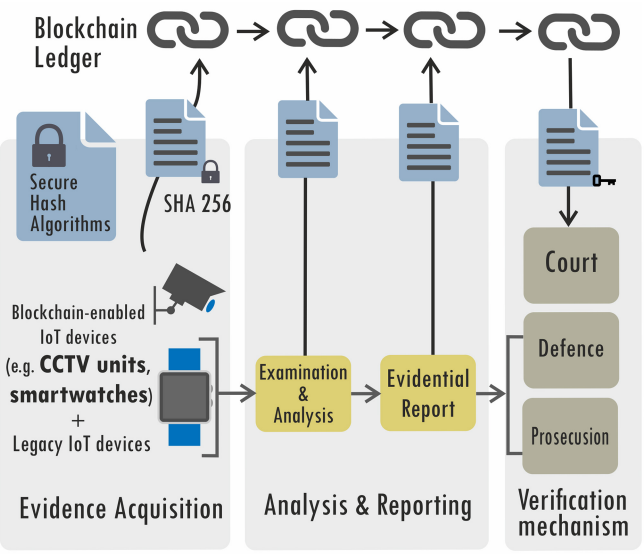

Fig. 7. Blockchain-enabled Digital Chain of Custody.

4) Securing Evidence Depending on the Deployment and/or the Service Model of the Cloud (PaaS, SaaS, IaaS): An important aspect in IoT Forensics is the availability of different paradigms for delivering cloud services. Based on the deployment model, the cloud could be Public, Private, Community or Hybrid, as shown in Figure 8 [9]. At the same time, there are three separate types of cloud services, based on the service model they provide.

Cloud platform services, or Platform-as-a-Service (PaaS), are currently the most popular model among all service models [118]. It is mainly for developers, offering them a framework they can build upon to test, deploy and customize applications by using standard programming languages, libraries, and tools supported within the providers' development platform [5]. In the PaaS model, the customers do not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, but the deployed applications and eventually the application hosting environment configurations. Examples include Heroku, Apache Stratos, Open Shift, AWS Elastic Beanstalk, Magento Commerce Cloud, Windows Azure, Force.com, Apprenda, and many more. According to Gartner's report on key trends in public cloud services [119], the PaaS market is going to double in size between 2018 and 2022.

Cloud application services, or Software-as-a-Service (SaaS), represent the second largest cloud market [120]. SaaS uses the Web to deliver applications that are managed by a third-party vendor and whose interface is accessed using thin clients like a Web browser or through an exposed program interface [5]. Well-known SaaS platforms are Google Apps, Salesforce, Dropbox, MailChimp, BigCommerce, ZenDesk, Workday,

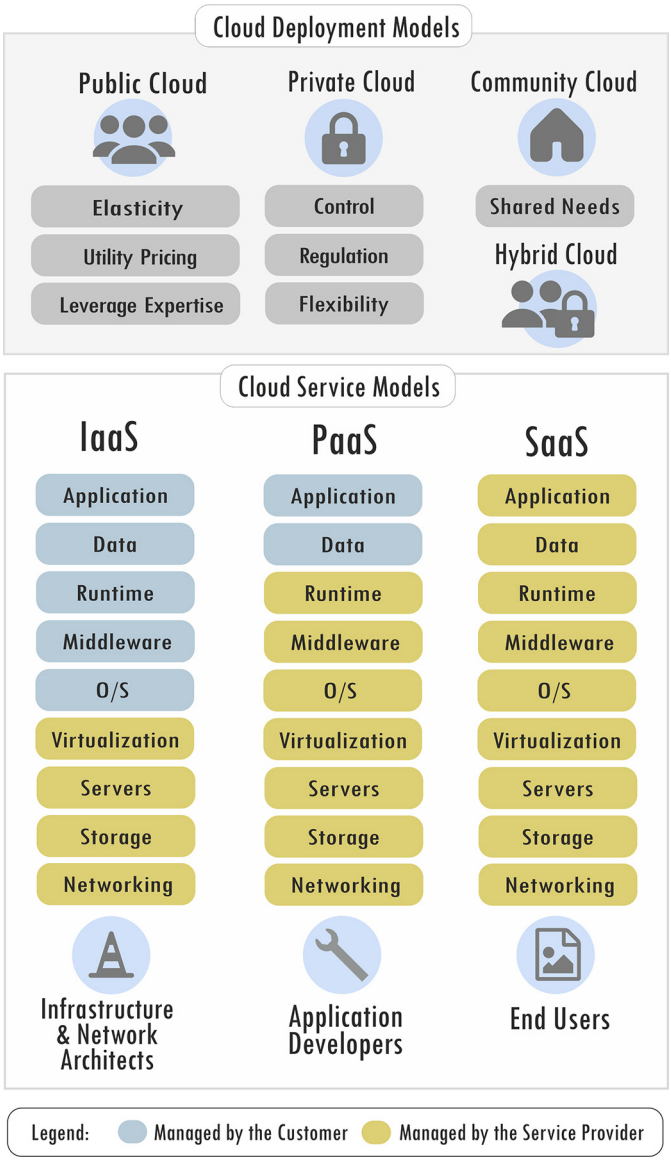

Fig. 8. Different Cloud types [97].

Hubspot, Concur, DocuSign, Slack, Citrix GoToMeeting, Cisco WebEx, etc.

Cloud infrastructure services, known as Infrastructure-as-a-Service (IaaS), are self-service models that offer computing power, basic storage, networks, and any other fundamental supporting resources to host virtual machines (VMs) [9]. Compared to SaaS and PaaS, IaaS users are responsible for managing deployed applications, data, runtime, middleware and OSes. Providers still manage virtualization, servers, hard drives, storage systems, and networking equipment [5]. Examples are Amazon Web Services (AWS) EC2, Cisco Metapod, Microsoft Azure, Joyent, Rackspace, Google Compute Engine (GCE), Digital Ocean, etc.

In summary, SaaS models provide a huge amount of integrated features, combined with a general high security level, or at least the responsibility for maintaining best security practices as part of the service [116]. When compared to SaaS, PaaS models have less integrated features, but allow developers to build and customize their own applications on the top of the providers' platform. By doing so, PaaS models trade extensibility for security capabilities. Similarly to PaaS, IaaS models offer generally less security functionalities, and expect that the protection of the operating systems, applications and contents will be managed by the customers [116]. From a security perspective, for all three cloud service models the following apply: the more flexibility the users are given, the more responsible they are for implementing and managing security capabilities.

From a forensics perspective, obtaining evidence in SaaS and PaaS primarily involves the service providers, while in IaaS forensics, investigators have to deal with both service providers and clients [31]. Therefore, investigating data of an IaaS user may require less restrictions, but in the case of SaaS the access evidence information might be minimal or completely missing [66].

5) Data Protection and Lack of Transparency in Cloud Services: When talking about cloud computing, storage and data protection are typically performed by the IaaS vendor. Since the quantity of providers is expanding, the user has been given plenty of opportunities to choose from (e.g., Google Cloud, AWS, Microsoft Azure, iCloud, and many more). Accordingly, the criteria that customers use to judge the quality of the service, is also changing. In 2018, a Delphi study [121] on the criteria for selecting a cloud service provider identified functionality and flexibility, but also legal compliance, contract, and geolocation of servers, as the top Quality-of-Service Attributes.

Most vendors declare that they encrypt users' data and archive it in the cloud. They may also have the financial capability to purchase the latest security software. However, some providers use common keys for storage encryption and archiving. According to Townsend's Definite Guide to Encryption Key Management Fundamentals [122], some organizations may also neglect other data protection issues such as: i) restricting the amount of information protected by a given key, ii) decreasing the amount of exposure if a certain key has been compromised, iii) limiting the time available for a physical, logical and procedural penetration attempt.

Besides data protection issues, the lack of transparency regarding the internal infrastructure of the cloud, poses another challenge in the investigation process. The cloud service providers (CSP) usually do not issue any information about the internal organization in order to preserve their reputation or to protect the data of their customers [104].

Furthermore, the physical equipment of the CSP may be placed or distributed among several other states or continents. If a user becomes involved in a criminal action, the access to the case-related information will be governed by the laws of the country where the CSP data center is located. All this could have unexpected consequences, as every state institution is allowed to acquire control over the data and freeze access to it, even if the investigation is not brought against the user from their own country of residence.

6) Data Storage Period in the Cloud: In most cases, the data storage period is determined by the provider of service. Legislation in different countries determines whether to store

data and for how long. In EU countries, this period can vary from 6 months to 10 years, depending on the type of data. For the U.S., the period is determined individually, however, there are suppliers located in countries where there is no legal provision for a minimum or maximum storage period, naturally creating preconditions for committing crimes.

D. Evidence Analysis and Correlation

1) End-to-End Analysis: Due to the fact that IoT nodes are continuously operating, they produce an extremely high volume of data. Keeping that in mind, it is understandable that the end-to-end analysis of the existing information exceeds the abilities of a single investigator or even of an investigating unit.

2) Data Origin: As vital part of any investigation process, the data provenance provides examiners with information about ownership and modification history of data objects. Unlike old-fashioned digital forensics examinations, in IoT Forensics there is less certainty about where the data came from, as well as who or what created and/or modified the data object. The extent to which data origin could be clarified depends on the cloud model [104] or the willingness of the vendor to co-operate with the authorities.

3) Time Lining and Limited Correlation of Evidence: The vast majority of IoT devices do not store any metadata (e.g., time and geospatial information, copyright information, creation and last modification date). This practically makes the correlation and logical consistency of evidence, collected from multiple IoT nodes, almost impossible. Lilis *et al.* [32] also outlined the unified time lining problem, in case of which different sources present different time zone references, clock skew/drift issues and timestamp interpretations. Without temporal information, investigators could only speculate on the causal links [29].

4) Legal Issues: Losavio *et al.* [103], provide an overview of present and future legal concerns in relation to IoT security and forensics. One of the main points refers to the conflicting legal guidance in case of cross-border crimes, including the absence of clear procedural and contractual agreements. A single file could be broken down into multiple blocks of data that are located on different nodes, and thereby fall within different jurisdictions. In the worst case, this leads to a breach of the law in the state where the forensic practice is actually carried out. The fact that each country has its own regulations, significantly increases the amount of time, the cost and the difficulty associated with a certain investigation [89].

E. Attack and Deficit Attribution

All investigation procedures aim to identify criminal parties. However, even if the evidence supports that a particular IoT node is the cause of the crime, this does not mean that the identified device will lead the investigators to the criminals.

1) Lack of User Information/IP Anonymity: Most of the cloud service providers maintain user-friendly policies and require minimal information when signing up for a service [123]. The adoption of IP obscurity tools, along with the above-mentioned easy-to-use features of many cloud systems, severely complicates the tracking down of a criminal [32], [89].

2) Sharing Resources and Identifying Liabilities: Traditional informational infrastructure is normally exploited by one user, while in case of cloud computing, multiple users share a physical server simultaneously. At the same time, physical servers could have many virtual machines that belong to different owners [2]. Thus, if one of the users performs an illegal activity, in a subsequent investigation, it would be very difficult to establish the truth. Investigators will have to examine not only the services used by a single customer, but a multi-tenant infrastructure, extensive sharing of resources and multiple potentially vulnerable interfaces [104].

Therefore, forensics professionals have to pay special attention when confirming the link between digital and physical identity. Incorrect assumptions could seriously bias the investigation process. For example, when analyzing verbal commands given to an Amazon Echo device, examiners have to find out if the person speaking was physically present or the command occurred through an audio conference [72].

It has to be pointed out that certain presence indication events (e.g., motion detection or door opening) do not necessarily reveal someone's identity. In the following example, the security alarm was deactivated before the house door was opened and a person entered the building. On one hand, the digital traces suggest that the home's owner issued the command and entered their home. On the other hand, the owner of the house could have also issued the command remotely and thereby, granted someone else an access to the building [72].

Finally, if the geolocation information extracted from a certain IoT device suggests that it was present at the crime scene in the moment of the incident, forensics examiners have to make sure that the device location and time settings were set accurately. Furthermore, the investigators should determine if the device was also used by another person at the same time [72]. Additionally, the fact that most of the modern companies let their employees use private devices for work, makes the task of identifying liabilities even harder [89].

F. Evidence Presentation

Presenting the findings of an IoT-centric case poses some new challenges. There are legal systems (e.g., the U.S. legal system) that require presentation of the evidence in front of a panel of jurors in the courtroom. Before being questioned and chosen by the judge and/or the attorneys, the potential jurors (also known as the "voir dire") were picked among the community using a reasonably random method. This means that the jury most probably has only basic understanding of cloud computing and forensics, based on the media or their personal experience with IoT technology. It would be a challenging task to explain to them the technicalities behind such a complex architecture in the very limited time of the trial [34], [124].

Finally, Hegarty *et al.* [95] note the fact that information aggregation and processing using analytic functions, could affect the structure of the data and alter its meaning [125].

Advanced presentation techniques are required, especially in such cases, when the data structure has been reverse engineered by the forensics practitioners [68].

IV. IoT Forensics Approaches and Frameworks

As illustrated in the previous chapters, in both theory and practice, there is no unique methodology to investigate in a digital environment. The same applies for IoT, where traditional investigative techniques have a very low success rate. There are various theoretical frameworks to choose from, even though they all adopt similar major stages [30]. In the end, the choice of approach mainly depends on the assessment of the investigative body.

On one hand, there are some considerable modeling attempts from the past, which unfortunately are unable to satisfy the requirements of a modern IoT-based investigation. On the other hand, there are several recent, experimentally derived models that are very specific and cannot serve as a comprehensive common IoT Forensics investigation model [94]. In addition, Harbawi and Varol [94] point out that the vast majority of modeling attempts lack proper experimental validation due to the unavailability of testing environments.

A. Overview of Past Digital Forensics Models (1995 - 2015)

Over the last 25 years, many forensic frameworks have been proposed and evolved based on the ever-changing technology, cybercrime attack patterns, experience on evidence admissibility, and government/public interest [40].

Section A in Table II presents in brief and chronological order, some of the basic digital forensics concepts introduced before the IoT paradigm was born (1995-2005). Hence, they were not designed to resolve the challenges mentioned in the previous Chapter. However, they are the foundation of the modern digital forensics discipline and have contributed to the development of the current theoretical frameworks.

Section B shows how the Digital Forensics has evolved over the past years (2005-2015) and has adapted to the challenges encountered in IoT and cloud computing. The current Chapter outlines some of the most well-established models from Section B, starting with the 1-2-3-Zones Approach (2013).

1) The 1-2-3 Zones Approach by Oriwoh et al. [54]: The 1-2-3 Zones Approach by Oriwoh *et al.* [54] may not be among the most recent developments, but it is perhaps the most cited theoretical framework in the Digital Forensics science. The authors offered a working method, through which it is easier to plan and systematize an IoT investigation.

The method reduces the complexity and the timing of investigations, which means that the authorities can focus their attention on substantial tasks and by doing so, achieve greater efficiency. The method divides the IoT Forensics into three zones represented in Figure 9.

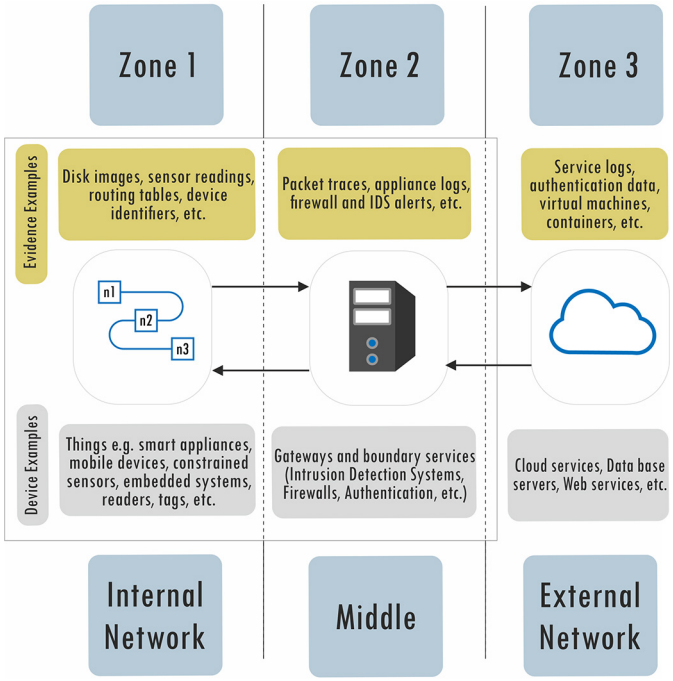

Fig. 9. Zones of Digital Forensics [54], [62].

• *Zone One:* The first zone covers the entire internal area consisting of hardware, software and networks. Here, the initial evidence is collected. One can also identify tag identities and their state. The investigator may decide to pay special attention to this area, if there is access to sites of forensic interest and/or open physical devices. In the absence of such devices, the Next-Best-Thing Triage Model may be applied (see 2).

• *Zone Two:* The second zone includes all the devices and software that connect the internal (Zone 1) to the external area (Zone 3). This area includes mainly public devices and infrastructure, intrusion prevention and detection systems, and network firewalls. During the investigation, it is necessary to gather maximum evidence by requiring assistance from the respective providers.

• *Zone Three:* The third zone covers all hardware and software that is outside of the network in question. According to [54], it includes evidence from:

i. All cloud, social network, Internet Service Provider (ISP) and mobile network providers' data;
ii. Internet and Web-based services, virtual online identities, edge network, internetwork evidence, device-based evidence, e.g., logs from Radio-Frequency Identification (RFID) tags and readers;
iii. Gateway or edge devices, etc.

2) The Next-Best-Thing Triage Model by Oriwoh et al. [54]: Another well-established Digital Forensics model is the Next-Best-Thing Triage (NBT) Model, also developed by Oriwoh *et al.* in 2013. This approach is highly likely to prove that data originated from a device that is no longer physically available. It helps the investigators to "arrange the puzzle" and gather enough evidence of a crime. The NBT model is successfully used in combination, or as basis, for the development of other forensics models and frameworks.

TABLE II
PREVIOUS RESEARCH ON THE DIGITAL FORENSICS PROCESS MODELS

	Name of the proposed approach or article	Specific	Complete	Readiness	DFaaS	Author/Year
A. Early Models **1995 - 2005**	Approach to Evidence in Cybercrime	Basic Digital Forensics Models which define the common successive phases of a typical investigation				Pollitt (1995)
	Scientific Crime Scene Investigation (SCSI) Model					Lee et al. (2001)
	Digital Forensic Investigation Model (DFIM)					Kruse & Heiser (2001)
	Digital Forensic Research Workshop (DFRWS)					Palmer (2001)
	Abstract Digital Forensics Model (ADFM)					Reith, Carr & Gunsh (2002)
	Computer Forensics - Secure, Analyze, Present (CFSAP)					Mohay et al. (2003)
	End To End Digital Investigation (EEDI)					Stephenson (2003)
	Integrated Digital Investigation Model (IDIP)					Carrier & Spafford (2004)
	Extended Model of Cyber Crime Investigation (EMCI)					Ciardhuáin (2004)
	Enhanced Digital Investigation Process (EDIP)					Baryamureeba & Tushabe
	Event Based Digital Forensic Investigation Framework					Carrier & Spafford (2004)
	General Digital Forensics Framework					Casey (2004)
	Hierarchical Objectives-based Framework					Beebe & Clark (2005)
B. Towards an IoT-adapted Framework **2005 - 2015**	Computer Forensic Field Triage Process Model (CFFTPM)	✓				Rogers et al. (2006)
	Integrated Digital Forensics Process Model		✓	✓		Kohn, Eloff & Oliver (2006)
	Common Process Model for Incident Response (IR) and Forensics			✓		Freiling & Schwittay (2007)
	Mapping Process of Digital Forensic Investigation Framework		✓			Salamat et al. (2008)
	Digital Forensic Model Based On Malaysian Investigation Process	✓				Perumal (2009)
	Generic process model for network forensics (GPMNF)			✓		Pilli, Joshi, & Niyogi (2010)
	Multi-component View of Digital Forensics		✓	✓		Grobler et al. (2010)
	The Digital Forensics Investigation Model (DFIM)	✓			✓	Ademu et al. (2011)
	Proactiv and Reactiv Digital Investigation Process			✓		Alharbi et al. (2011)
	The Systematic Digital Forensic Investigation Model (SDFIM)	✓	✓			Agawal et al. (2011)
	Integrated Conceptual Digital Forenic Framework for Cloud Computing		✓			Martini & Choo (2012)
	Computer Forensic Workflow Management and Processing using Cloud				✓	Wen et al. (2013)
	Enhanced Systematic Digital Forensic Investigation Model (ESDFIM)		✓			Kyei et al. (2013)
	Next-Best-Thing (NBT) Triage Model; 1-2-3 Zones Approach		✓	✓		Oriwoh et. al. (2013)
	Harmonized Process Model for DF Investigation Readiness		✓	✓		Valjarevic & Venter (2013)
	The Hybrid Model		✓	✓		Vlachopoulos et al. (2013)
	Integrated Digital Forensic Process Model		✓			Kohn et al. (2013)
	Advanced Data Acquisition Model (ADAM)		✓			Asams et al. (2014)
	Digital Forensics as a Service				✓	van Baar et al. (2014)
	Forensics-aware IoT Model (FAIoT Model)			✓		Zawoad & Hasan (2015)
	Domain Specific Cyber Forensic Investigation Process Model	✓				Satti & Jafari (2016)
	Top-down forensic approach methodology for IoT		✓			Perumal et al. (2015)
C. Recent Advances **2016 - 2019**	Generic digital forensic investigation framework for IoT (DFIF-IoT)		✓	✓		Kebande & Ray (2016)
	IoT Forensics Model for Data Reduction					Quick & Choo (2016)
	Mobility Forensics Model	✓	✓			Rahman et al. (2016)
	Field Processing Model	✓			✓	Hitchcock et al. (2016)
	Application-Specific Digital Forensics Investigative Model in IoT		✓			Zia et al. (2017)
	Last-on-Scene (LoS) Algorithm		✓			Harbawi et al. (2017)
	Real-Time Approach for IoT Forensic			✓		Zulkipli et al. (2017)
	Privacy-aware IoT-Forensic Model (PRoFIT)	✓		✓		Nieto et al. (2017)
	Forensics Framework for Cloud Computing		✓	✓		Alex & Kishore (2017)
	Forensic State Acquisition from Internet of Things (FSAIoT)		✓			Meffert et al. (2017)
	DF Model of Smart City Automated Vehicle Data Investigation	✓				Feng et al. (2018)
	IoT Dots: A Digital Forensics Framework for Smart Environments	✓				Babun et al. (2018)
	Public Digital Ledger Based Investigation Framework (Probe/FIF-IoT)	✓				Hossain et al. (2018)
	Forensic Investigation Framework for Smart Home Environment	✓				Goudbeek et al. (2018)
	Framework for IoT Data Acquisition and Forensics Analysis		✓			Chi et al. (2018)
	Blockchain-based decentralized framework for IoT Forensics	✓		✓		Ryu et al. (2019)
	A Holistic Forensic Model for the Internet of Things		✓	✓		Sadineni et al. (2019)
	Video-Based Evidence Analysis and Extraction in DF Investigation	✓				Xiao et al. (2019)
	Trust-IoV: A Trustworthy Forensic Investigation Framework for IoV	✓			✓	Hossain et al. (2019)
	A comprehensive UAV/Drone Forensic Framework	✓				Renduchintala et al. (2019)

3) Top-Down Forensic Methodology by Perumal et al. [126]: Perumal *et al.* [126] proposed a new IoT forensic model that has been developed on the basis of the work of Oriwoh *et al.* and their 1-2-3 Zones model [54]. The top-down approach includes device identification, location finder represented by zones, and triage examination to deal with specific digital evidence wherever it resides within the zone.

4) FAIoT: Forensics-Aware Model for the IoT by Zawoad and Hasan [124]: In 2015, Zawoad and Hasan [124] presented a conceptual model for executing Digital Forensics in the IoT infrastructure with a centralized trusted evidence repository to ease the process of evidence collection and analysis. In order to ensure the evidence reliability, the proposed evidence repository applies a secure logging schema, introduced in [127]. To summarize the idea, Secure-Logging-as-a-Service [127] stores and preserves proof of past virtual machines' logs (e.g., network logs, registry logs, sensor readings). Thus, SecLaaS protects the integrity of the logs via a hybrid (asymmetric-symmetric) encryption, and ensures the confidentiality of the cloud users. Law enforcement agencies could access the evidence material via secure read-only APIs.

B. Overview of the Recent IoT Forensics Theoretical Frameworks (2016-2019)

Although the field of IoT Forensics research is relatively new, there are already some promising modeling attempts (see Section C in Table I).

1) DFIF-IoT: A Digital Forensics Investigation Framework by Kebande and Ray [128]: The Digital Forensics Investigation Framework for IoT (DFIF-IoT) is a generic framework proposed by Kebande and Ray [128] in 2016. A major advantage of this approach is that it complies with ISO/IEC 27043: 2015 [129], a still valid, internationally recognized standard on incident investigation principles. Later on, Kebande and his colleagues presented the IDFIF-IoT, an Integrated Digital Forensics Investigation Framework [130]. This model is capable of analyzing Potential Digital Evidence (PDE) generated by an IoT-based ecosystem, and could be understood as an extension of the Digital Forensics Investigation Framework (DFIF-IoT), initially-presented in [128].

In both works, the researchers have recognized the need for standardized mechanisms for evidence extraction and reporting [131], [132]. Another advantage of the models is that they are easily applicable to various IoT environments. At the same time, they lack low-level details that would enable their adaption to different scenarios without changing any main components or processes.

2) The Last-on-Scene (LoS) Algorithm by Harbawi and Varol [94]: In 2017, Harbawi and Varol [94] provided an improved theoretical framework for IoT Forensics that copes with the evidence acquisition issues. Their LoS Algorithm states that the device which represents the last node in the communication chain must be the first one investigated. The benefit of this theoretical concept is that it limits the scope of investigation. In conjunction with the NBT model (see Section A), the process of evidence identification starts at Zone 1 and is continuously applied within all subsequent zones.

3) FSAIoT: Forensic State Acquisition Model for IoT Devices by Meffert et al. [115]: Another model that focuses on the evidence acquisition process was proposed by Meffert *et al.* [115]. Their FSAIoT framework consists of a centralized Forensic State Acquisition Controller (FSAC) employed in three state collection modes: controller to IoT device, controller to cloud, and controller to controller.

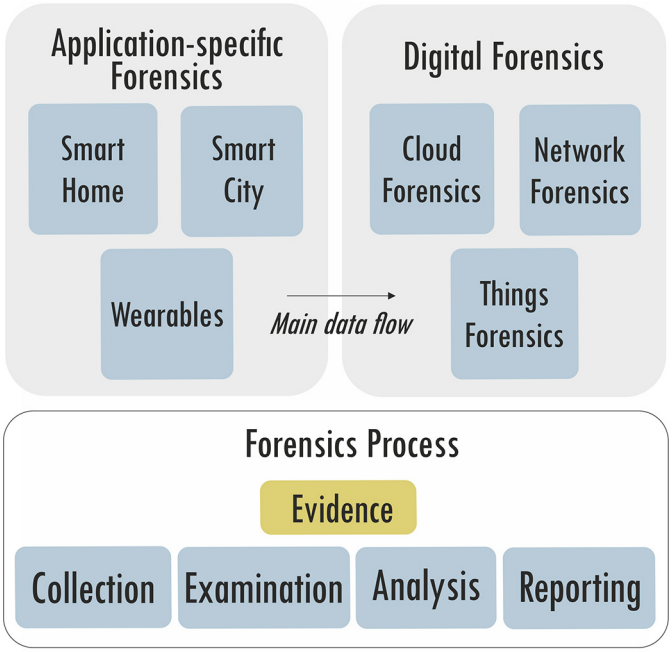

Fig. 10. Components of the Application-Specific Digital Forensics Model by Hossain *et al.* [12].

4) Application-Specific Digital Forensics: Zia *et al.* [133] offered a new forensic model that consists of three independent components: application specific Forensics, Digital Forensics and Forensics Process. Each of the above-mentioned categories comprises several other topics (see Figure 10). The application-specific forensics for example, is conceptualized based on the three major domains in IoT: Smart Home, Smart City and Wearables.

Smart home systems are gaining popularity, which makes them a common topic among forensics practitioners and researchers. In a recent work, Akatyev and James [65] chose to focus on near-future interconnected heterogeneous smart home environments and develop their User-Centric IoT (UCIoT) system. Abie [76] focuses on another field of application, namely Healthcare Ecosystems. The authors propose a cognitive framework that is supposed to address the emerging cyber-security and privacy threats to CPS-IoT (IoT-enabled Cyber Physical Systems) and critical infrastructure systems.

5) IoTDots (A Digital Forensics Frameworks for Smart Environments): Babun *et al.* [134], [135], proposed their IoTDots model that automatically analyzes and modifies smart applications to detect and store forensically-relevant information inside the apps. The framework consists of two main components: Modifier (ITM) and Analyzer (ITA). After the ITM detects the relevant data, it is sent to a secure Database (ITD). In a second step, IoTDots applies data processing and machine learning in order to detect valuable digital evidence from smart devices, apps, or user activities.

6) Privacy-Aware IoT Forensics: Extracting evidence data without violating users' right of privacy could be especially challenging in the IoT context. Therefore, Nieto *et al.* [55], [56] developed a model (PRoFIT) that takes privacy regulations into consideration by incorporating the ISO/IEC 29100:2011 regulation (today revised and published as [136]) throughout the whole forensic investigation process. The proposed framework stresses the importance of collaborating with nearby devices to gather information and reconstruct the context of the crime scene. In fact, the proposed model is adapted to make it compliant with the previously mentioned concept of the "digital witness" (see Section Securing the Chain of Custody in Section III).

Verma *et al.* [108] described another automated, privacy-preserving framework that utilizes machine learning in order to locate Forensically Irrelevant Files (FIF) and protect them (see Section Privacy and ethical considerations by accessing personal data in Section III). Furthermore, it uses intelligent techniques to determine the relevance degree, as well as the level of privacy, for all Forensically Relevant Files (FRF). At first, the investigation unit gains access to only the most applicable files (e.g., a list of 20 or 50 files). The next bunch of files is delivered at the explicit request of the investigator, and only after examining the previously presented file material. Clearly, the privacy protection via such filtration is not a complete solution. Nevertheless, it preserves privacy in a way that does not affect neither the integrity of the evidence nor the investigation process itself.

7) A Holistic Forensic Model for the IoT by Sadineni et al. [36]: In 2019, Sadineni *et al.* [36] present an integrated forensic model for the IoT that is based on the current ISO/IEC 27043 international standard. The proposed framework aims to cover the entire forensic process, and therefore, consists of three main phases: forensics readiness (proactive), forensic initialization (incident) and forensic investigation (reactive).

8) Blockchain-Based Investigation Frameworks: The work of Atlam *et al.* [137] suggests that moving the Internet of Things into the decentralized path, may be the key to managing the huge number of cyber-attacks. Furthermore, the immutable, distributed nature of the blockchain technology may also suit the demands of the IoT Forensics. Digital evidence could be collected and updated in the ledger where the immutability of the blockchain will ensure its validity and unchanged character. The forensically relevant information could be reliably accessed by the investigating unit from any of the nodes, at any time. Therefore, blockchain could be used to timestamp and maintain the integrity of the digital evidence [36].

Users, device manufacturers, cloud service providers, law enforcement agencies, forensics professionals, as well as all other participants in the IoT-based ecosystem could maintain a copy of the ledger. Hence, the evidence storage could not be deleted or manipulated by a single control entity, and the problem of the "single point of failure" is eliminated [138].

Consequently, a wide variety of research contributions [106], [107], [139], [140] have been presented to cope with the forensics challenges by using blockchain technology. Ryu *et al.* [57] for example, proposed a whole blockchain-based decentralized framework for IoT Forensics. Lone and Mir [58] implemented Ethereum Blockchain to secure the Chain of Custody, while Banerjee *et al.* [141] demonstrated how to track changes made to IoT device firmware, and automatically restore the original data in the event of tampering. Some other scholars such as [47], [142], [143] presented blockchain-based forensic applications for connected vehicles (see Section Mobility Forensics Frameworks).

Hossain *et al.* [138] proposed a forensic framework (Probe/FIF-IoT), which employs a public digital ledger to find facts in criminal incidents within different IoT-based systems. It stores evidence in a form of interactions between devices, users, and cloud (e.g., Things to Users, Things to Cloud, and Things to Things interactions) and keeps them secure in the distributed blockchain network. According to the authors, the system is capable of providing integrity, confidentiality, anonymity, and non-repudiation of the publicly-stored evidence. Furthermore, Probe-IoT offers a scheme to verify the authenticity of the evidence gathered during the investigation.

9) Video-Based Evidence Analysis: In 2019, Ericsson [144] predicted that video traffic will grow by around 34 percent annually, and by 2024 will account for nearly three-quarters of the mobile data traffic. Moreover, according to the same Ericsson's Mobility Report, augmented reality and streaming of 360-degree video are expected to be another significant factor in mobile traffic growth. Due to the increased amount of smartphone video data, as well as the popularity of low-cost surveillance systems, visual material is progressively being used in the Digital Forensics discipline.

As a result, fields like motion detection, body and face recognition, gait recognition, cross-pose recognition, and comparative image analysis, have been widely researched in the past few years. Nevertheless, some challenges still remain. Closed-circuit television (CCTV) systems, for example, export footage in different formats and often need to be converted to other, suitable for analysis formats. This may lead to information loss or lowering the quality. Therefore, the forensics discipline needs video analysis frameworks that employ efficient image enhancing algorithms for low quality footage. An approach that addresses the aforementioned issue was presented by Xiao *et al.* [145]. Their work introduces a video enhancement algorithm based on contrast limited adaptive histogram equalization (CLAHE). While some researchers like [146] focus on the image/video sources identification, others propose forensic approaches to automatically analyze a huge volume of video files. Horsman [147] for example, presented a procedure which identifies and reconstructs online cached video stream data from platforms like YouTube, Facebook, Twitter, and WeChat.

Clearly, video-centered cases depend on the quality of the footage. Unfortunately, the majority of the recordings (e.g., security and monitoring cameras) differ from gallery images because of their low resolution quality, angle of view, color, data rate, etc. In order to guarantee a precise forensic identification process, new techniques for video quality improvement need to be developed, for example advanced robust evidence extraction and subject detection methods [145]. Intelligent

techniques like deep learning could also improve and shorten the evidence identification phase. Especially in the domain of video-based facial recognition, poor video quality could significantly impact the investigation level and bias the investigation course. Because of that, forensics professionals are expected to use an extended amount of available forensics techniques, such as facial ageing, marks, near-infrared face recognition or forensics sketch recognition, etc. [145]. With the growing number of devices and data volume, there will be an even greater need for further in-depth authenticity examinations and validation procedures [68].

10) Mobility Forensics Frameworks: Mobility forensics integrates vehicular ad hoc networks (VANETs), Internet of Things and mobile cloud computing. It is a complex field that aims to deal with the challenges of highly dynamic, distributed infrastructures. The assembly of interconnected devices include smart autonomous vehicles and unmanned aerial vehicles (e.g., drones), various mobile devices, even military equipment [45].

As already illustrated in Section III, conventional digital forensics tools are insufficient in IoV environments due to the mobile, dispersed nature of the nodes. A smart car for example, might join or leave a certain network at any point, anytime. Furthermore, besides the common risks to security and confidentiality, the autonomous traffic is prone to attacks against the road side units (RSUs). Since RSUs are usually left unattended, a potential attacker might try to tamper with the RSUs and disable the forensics support [47]. This could significantly slow down the investigation, unless the RSUs are embedded with tamper-resistant packaging to protect them from the anti-forensics techniques [47].

Several factors must be considered before designing a mobility-compliant forensics model. One of them is the exponentially increasing demand for data traffic. Since the major part of the IoT communication is conceptualized over wireless cellular technologies, the new advancements in the field will reflect and shape the near-future mobile forensics as well.

The work of Al-Turjman *et al.* [25], shows that the scientific community and mobile operators are searching for new solutions that could boost communication capacity and coverage, and address the device heterogeneity and the explosive growth in mobile data traffic (e.g., mobile video). The authors recognize the forthcoming 5^{th} generation mobile network as the center of the emerging IoT communication technology. Besides public safety and emergency handling, 5G networks are expected to support other important features related to industrial control applications and Vehicle-to-X (V2X) communications (see Figure 11). According to Al-Turjman and his colleagues, such ultra-reliable Machine Type Communications (u-MTC) could make a big difference between 5G and previous mobile network generations. In general, users could expect higher data rates, enhanced coverage, increased number of connected devices, and low latency [25]. One particular technique that promises to meet the requirements of rural or densely populated areas, is the use of small cells (e.g., femtocells). The authors in [25], consider the deployment of Femtocell Base Stations as a way to provide high data rate services in a less costly manner. From a forensics point of view, femtocells could play an important role during an investigation in urban environments since they could be used in public transportation systems (e.g., in trains and busses), in order to offload the traffic from saturated macrocell networks [25].

Another interesting aspect in the context of mobility forensics comes from Lohmann [148]. Their work elaborates on the theme of civil liability, concerning self-driving vehicles. According to the authors, under strict liability regimes, the vehicle holders will remain liable for accidents caused by automated cars. However, due to the increased use of vehicle automation, a shift in liability from the users towards the manufacturers may occur [148]. While the total number of the accidents will be expected to decline, users will be particularly sensitive to accidents that occurred due to a technical malfunction during the automated decision-making process. This goes back to the fact that the question "who was driving – man or machine", is often overexposed in media and politics. From a psychological point of view, people also tend to have intense emotional reactions towards disruptive technologies, especially regarding safety innovations. After all, the social acceptance of autonomous vehicles lies on the premise that autonomous vehicles will, on the whole, be safer drivers than people [149]. Therefore, in the context of IoV-centered investigations, forensics professionals have to pay special attention not only to the evidence extraction and analysis process, but also during the step of attack and/or deficit attribution [29].

Because of all the aforementioned challenges, the forensics practice will need efficient, mobility-compliant security algorithms, and a forensic model specifically designed for smart autonomous vehicles. In the recent couple of years, blockchain-based decentralized trust management systems seem to be one of the major trends not only in the broad IoT domain, but also explicitly for IoV security and forensics. Oham *et al.* [143] for example, proposed a blockchain-based framework for autonomous vehicles that includes a liability model and provides untampered evidence for deficit attribution. Another model proposed by Rahman *et al.* [150] presented a blockchain-based mechanism that can support security and privacy-oriented spatio-temporal smart city services, such as sharing economy, smart contracts, and cyber-physical interaction in the IoT context.

In order to cope with the issue of trustworthy data collection from distributed IoV infrastructures, Hossain *et al.* [47] presented their Trust-IoV model. It consists of two parts: Forensics Gateway (FG) and IoV-Forensic Service (IoV-FS). The Forensic Gateway collects information from the distributed and decentralized entities such as smart cars, roadside units, smartphones, and cloud IoV services. Then, the collected digital evidence is securely stored in the IoT-Forensic Service. To ensure the confidentiality and integrity of the digital evidence, the authors propose to use an Electronically Signed Evidence (ESE) module which exposes read-only APIs to provide access to the evidence material.

Aiming to provide a full and comprehensive systematization of information and evidence gathering, Rahman *et al.* [151] suggested a set of six main questions that should assist the

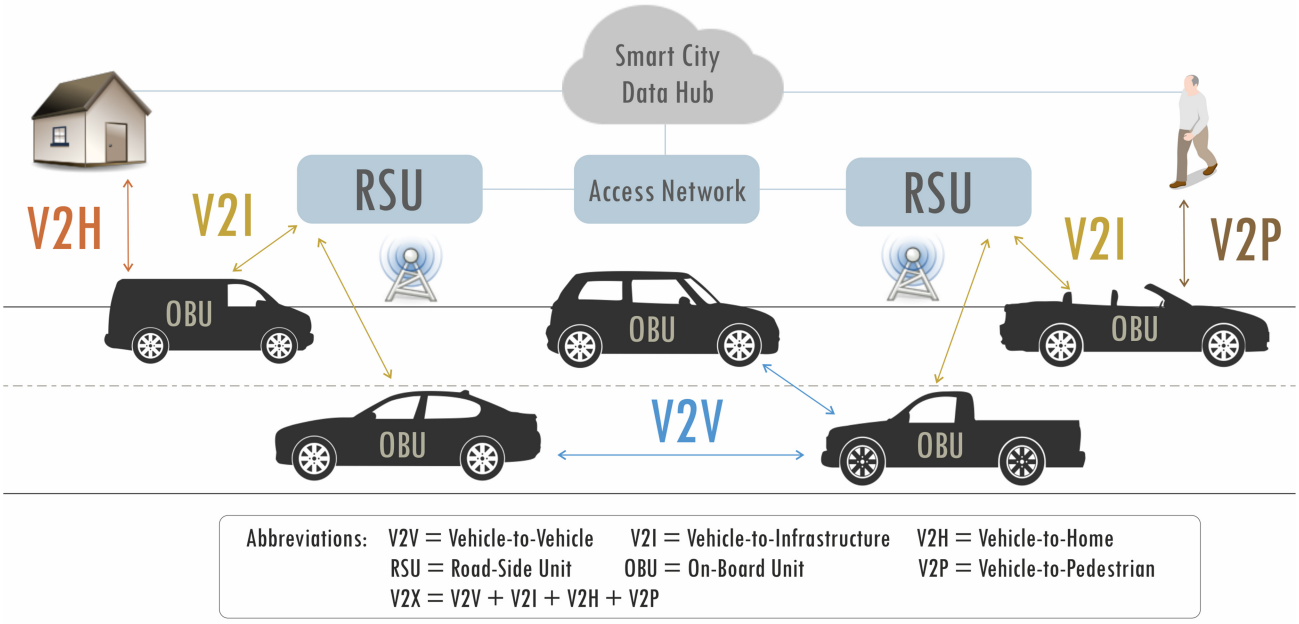

Fig. 11. Vehicle-to-X communication [45].

examiners in the field of IoT mobility forensics. While answering these questions, forensics professionals should also take into account the challenges associated with cloud computing (see Section The Cloud Forensic Problem(s) in Chapter III). Therefore, the set presented in Figure 12 should be completed with three additional questions: i) How much can we trust data extracted from IoT devices? ii) How do changes made by the attacker affect the forensics analysis? iii) How can we prevent or detect such manipulation?

In 2018, a new concept called Incentives-based Vehicle-Witnesses-as-a-Service (IVWaaS), was described in [152]. The presented architectural framework employs vehicles moving on the road as witnesses to designated events. Another comparable idea is the Pics-on-Wheels service by Gerla *et al.* [85]. Similar work has also been done by Hammoudi *et al.* [153] who presented a vision-based, cooperative vehicular embedded system for enhancing road monitoring services. All three frameworks can be used in criminal investigations (e.g., car lifting), traffic and route management, and fine-grained cooperative awareness models. Main difference between the approaches is the incentives mechanism introduced by [152]. It is called privacy-aware proportionate receipt collection (PPRC) and has the aim to boost the user's participation in the data gathering process.

A less explored branch of the mobility forensics discipline is the UAV Forensics. UAVs, otherwise called drones, are often misused for illegal activities because of their well-known ability to get close to critical targets. In the past three years, the UK Airprox Board documented nearly 30% increase in the number of incidents involving drones and civil aircrafts [154]. A recent example was the Gatwick Airport drone incident that shut down England's second-busiest airport for three consecutive days, causing major disruption and affecting approximately 140,000 passengers [155]. The increasing number of such incidents motivated airports like Gatwick and Heathrow

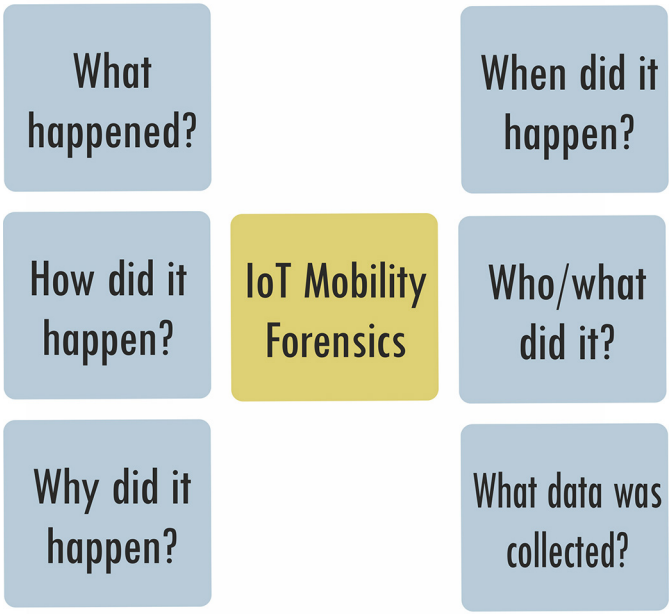

Fig. 12. IoT Mobility Forensics Model by Rahman *et al.* [151].

to purchase expensive anti-drone equipment, but it also accelerated the development of frameworks for the post-flight investigation of drone activities.

In a paper from 2019, Renduchintala *et al.* [50] proposed a comprehensive drone forensic model that combines both hardware/physical and digital forensics. The researchers applied a novel approach that could analyze the unabridged flight plan of a given UAV, and thereby determine if its route was in compliance with the regulations (for example, avoiding No Drone Zones close to the airports). To achieve that, Renduchintala *et al.* visualized the UAV's flight information and provided a 3D representation of its path using Google

maps. Another work by Jain *et al.* [51] analyzed the UAVs' architecture and came with a generic drone forensic model. It consists of twelve linear phases that should be considered as a waterfall model, and include examining drone components such as camera, Wi-Fi, memory card, as well as operations like checking for customization and searching for paired devices.

Last but not least, a recent work by Salamh *et al.* [156] suggests an enhanced model of Drone Forensics, as well as an Incident Response plan (DFIR), covering storage mechanisms used by three different types of drones: DJI Phanthom 4 Pro; Typhoon H; and DJI Mavic Pro. The scholars in [156], pointed out that when it comes to digital forensics investigation, the metadata inside the media files represent valuable evidence material. Furthermore, the work discusses drone disrupted denial of service attacks (3DOS), along with some possible anti-forensics techniques that could be implemented to alter digital evidence associated with drones.

V. Open Issues and Research Directions

Although machine-to-machine communication is vividly portrayed, there are still many uncertainties and unexplored areas. The following section addresses the most substantial ones among them.

A. Towards Standardization and Certification in IoT Forensics

Digital Forensics, and particularly IoT Forensics, has to deal with a huge assortment of devices, as well as with a vast number of formats and manufacturers. Establishing standards for such rapidly involving technology, with a huge and heterogeneous group of stakeholders, is not an easy task [91]. Different Standard Bodies (CEN, UNECE, CENELEC, ETSI) and safety or security labs (EuroNCAP, KEMA, CLEFs, Underwriters' Labs, ENCS, etc.) aim at providing infrastructure for forensic sciences by addressing quality issues.

One of the first steps towards knowledge exchange and mutual agreements within the Digital Forensics took place in 1998, when the European Network of Forensics Science Institutes (ENFSI) created the Forensics Information Technology Working group [40]. Two years later, the DFRWS research conference identified particularly relevant digital forensics topics and proposed one of the first comprehensive roadmaps in the field. In the United States, the Scientific Working Group on Digital Evidence (SWGDE) was created in 2002 with the aim to develop *"standards and guidelines related to information of probative value that is stored or transmitted in binary form"* [157]. During their tenure of office, SWGDE has published more than 50 best-practice guidelines, some of which have been adopted by the G8 [73], [91].

Additionally, there are many directives and regulations that ensure the safety of products and services offered on the European market, including IoT devices and services. The examples comprise: Product Liability Directive (85/374/EES); Regulation 428/2009; Directive 2009/EC/72; The NIS Directive (2016/0027 COD); General Data Protection Regulation (2016/679), etc. [158].

With regard to the digital forensic investigations in Europe and worldwide, the following standards have been developed and implemented so far:

ISO/IEC 27035 – Part 1: Principles of incident management [159], to be replaced by ISO/IEC WD 27035-1 [160]; Part 2: Guidelines to plan and prepare for incident response [161], to be replaced by ISO/IEC WD 27035-2 [162];

ISO/IEC 27037 – Guidelines for identification, collection, acquisition and preservation of digital evidence [163];

ISO/IEC 27038 – Specification for digital redaction [164];

ISO/IEC 27040 – Storage security [165];

ISO/IEC 27041 – Guidance on assuring suitability and adequacy of incident investigative method [166];

ISO/IEC 27042 – Guidelines for the analysis and interpretation of digital evidence [167];

ISO/IEC 27043 – Incident investigation principles and processes [129];

ISO/IEC 27050 – Electronic discovery [168], to be replaced by [169];

ISO/IEC 30121 – Governance of digital forensic risk frame work [170];

ISO/IEC 27017 – Information technology – Security Techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services [171];

ISO/IEC 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors [172];

ISO/IEC 27031 – Guidelines for information and communication technology readiness for business continuity [173]. This standard will be soon replaced by ISO/IEC WD 27031 [174] which is currently under development;

ISO/IEC WD 27030 – Guidelines for security and privacy in Internet of Things (IoT), currently under development [175];

ISO/IEC DIS 20546 – Information technology – Big data – Overview and vocabulary [176];

ISO/IEC TR 20547-2 – Information technology – Big data reference architecture; Part 2: Use cases and derived requirements by [177];

ISO 22320 – Security and resilience – Emergency management – Guidelines for incident management [178].

The most relevant standards for investigation of digital incidents are summarized in Figure 13. By taking a closer look at the presented figure, it becomes clear that there is an undeniable need for more explicit guidelines, especially referring to the phases of evidence identification, collection and preservation.

Karie *et al.* [53] criticize some of the existing standards (e.g., ISO/IEC 27043: 2015) because of the way the report generation step is described. According to the authors, the current version of ISO/IEC 27043 is not comprehensive enough, and does not cover the entire forensic process adequately. For example, it states that the results from the evidence interpretation process, need to be compiled and presented in a form that can be printed on paper. Nevertheless, some previous research [179], suggests that visual presentation approaches (e.g., multimedia) should be also considered, explicitly

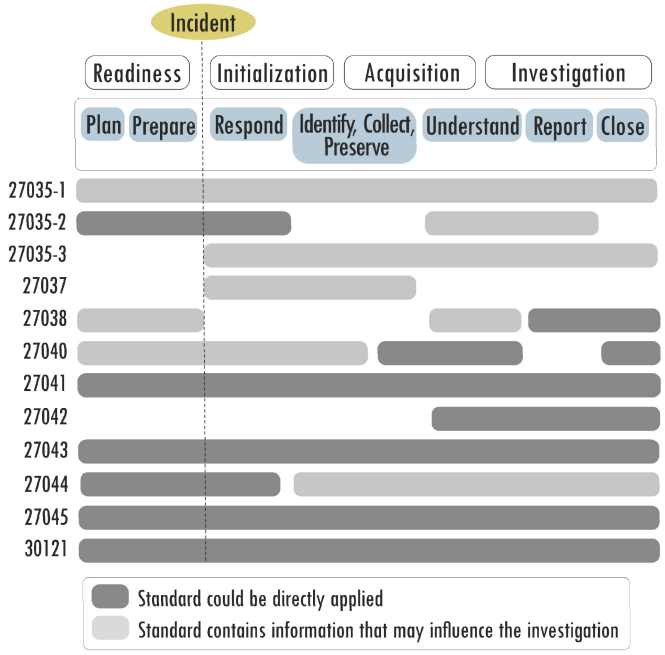

Fig. 13. Applicability of standards to investigation process classes and activities [201].

in cases that involve immensely complex technical terms.

Finally, it should also be considered that the process of changing current regulations is a very complex one, and cannot keep pace with the industry and the insurance companies [158]. A recent example for updating the current legislation is the new General Data Protection Regulation (GDPR) that came into effect on the 25 May 2018. The primary objective of the GDPR is to encourage companies to protect their clients' personal data, as well as to penalize the firms with inefficient security and privacy measures [180]. The regulation applies to every single organization that deals with data of EU residents.[3] Failure to achieve compliance could result in fines greater than €20 million or 4% of global turnover [180].

From a forensics point of view, an interesting fact is what the GDPR stipulates in case of a security breach. In 2012, the global average time required to identify a data breach was 6 months [110]. By 2016, it improved to 4 weeks. According to a study [181], conducted by the Ponemon Institute on behalf of IBM, the global average time now lies at 197 days. To compare, companies must be able to report a breach within 72 hours of discovery in order to be GDPR-compliant.

Many firms believed that achieving compliance will not pose a huge challenge, since the GDPR states that a breach must be reported "within 72 hours of discovering", and not "within 72 hours of occurring" [182]. However, reporting the breach should also include information about what were the attackers aiming at, what was tampered with, which data was stolen and which was deleted [182]. At this point, two main challenges arise. First, one could question the companies' motivation to *discover* the security breach as soon as it *occurs*. Second, in case of cloud systems, compliance in terms of detailed report may be an impossible requirement since intruders could have deleted not only the forensic trail, but anything else they desired (see Section The Cloud Forensic Problem(s) in Chapter III). In this case, it will be impossible to find out which records have been compromised by being read, changed or deleted from the system [110].

Obliged by the GDPR, companies rushed to get explicit consent from the customers to hold their data. Furthermore, users now have the right to own their personal data, as well as the opportunity to access and delete it. In addition, users can find out how and why their data is being processed, and get a free electronic copy of it. Overall, the EU GDPR gives individuals eight fundamental rights related to the Protection of Personal Information (PPI). Nonetheless, as important as these rights are, some of them are also posing new challenges from a forensic perspective.

For example, the possibility for users to erase information is not clarified enough – will the users' information be deleted in logs and backups as well? Normally, personal information is not supposed to be stored in logs. However, if so, the request to delete a user will mean to alter the logs [183]. This on the other hand, will turn the logs into invalid evidence material because they have already been changed.

B. Data Processing via High-Performance Computing

The increased number of cybercrimes has urged researchers to focus on the effectiveness of the current generation forensic tools [89]. According to Lillis *et al.* [32], the processing speed of the available digital forensic tools is inadequate for the average cases. This is due to two major factors. On one hand, it is the lack of explicit performance requirements. On the other hand, there are developers who prioritize reliability and correctness over processing. The authors propose that using Optimal High-Performance Computing (HPC) wherever possible, could reduce computational time and have a positive impact on the investigation process in general. HPC advantages could be especially visible during the time-consuming phases like pre-processing, analysis, reporting, etc. [32].

C. Forensics Tools Limitations

It is vital to document the tools and techniques used while conducting an investigation, especially if there are tools that have not been trialled-and-tested in depth yet. Additionally, the investigating unit should include information about the model and/or version number of the programs used. Furthermore, to ensure forensic soundness, investigators should document and justify any decision to omit certain steps or inapplicable procedures (see Section Securing the Chain of Custody in Chapter III), as well as any known limitations of the tools used [53].

Usually, investigations are carried out using commercial digital forensics tools [184]. However, a major drawback of these tools is the lack of transparency. In other words, because manufacturers are reluctant to reveal the source codes, the

[3]The U.K. Government has indicated that GDPR will also apply in a post-Brexit scenario [200].

exact mode of operation of commercial forensics tools remains unknown [184]. Unlike commercial solutions, open source forensics tools offer some verifiability. At the same time, gaining command of them requires more training [185].

D. Error Mitigation Analysis

In essence, error mitigation analysis involves testing and validation of digital forensics tools. By analyzing a specific IoT Forensics case, this approach provides what Casey [73] calls a *quality assurance framework*. Basically, it is a method to study each potential source of error, be it human or technology. In a further step, the error mitigation analysis is used proactively, in order to take precautions, and thereby reduce the risk of future mistakes. According to Casey [73], current limitations of this approach are that it does not address possible human observer bias, or algorithmic bias in an automated forensics analysis.

E. Data Inclusion and Exclusion Criteria

Data acquisition plays a crucial role in every forensics investigation. Yet not all of the collected and analyzed information could be (or needs to be) included in the final evidence report [53]. In order to decide which information is relevant and which is not, the investigating unit has to create and apply clear inclusion/exclusion rules. Finally, the content that was not included has to be archived. Besides secure storage location, there should be also a legally pre-defined archiving time period [53].

F. Automation and Forensics Intelligence

Eventually, there have been many attempts to integrate artificial intelligence (including machine learning and deep learning approaches) in the security and digital forensics practices. Intelligent methods have been applied for anomaly detection [59], forensics video analysis [145], rule extraction [186], intrusion classification [177]. Buczak and Guven [187] for example, presented a literature survey, which discusses application areas of different intelligent methods, with focus on data mining techniques for intrusion detection.

Automated evidence collection and analysis on a large scale is being promoted, because if correctly applied, it could decrease the occupancy of resources involved, for example, the amount of time, manpower, and money spent on a certain investigation [66], [100]. In particular, automation increases the forensic soundness during the evidence collection procedure due to the fact that it makes this step repeatable and thereby, reduces the human error dependency [62]. Besides verifying the acquisition process, automated forensics could also reduce the operational overhead in cases where investigators have to deal with a huge amount of evidence sources, a typical IoT Forensics case [62].

Apart from the above-mentioned advantages, proactive and automated forensics have raised some social and ethical issues [35]. Critics believe that automation could deteriorate the knowledge of the forensics professionals, and herewith the general quality of the investigations [66]. Besides the potential overreliance on automation tools, the forensics practitioners point out that the further they get away from the manual handling, the greater the chance for errors and evidence omission [184].

At this stage, there are also some technical challenges associated with the data processing time. In order to be able to track different devices located on various places and provide real-time insights, automated IoT forensic tools require improvement in terms of performance [35].

G. Forensics-by-Design and/or Digital Forensics-as-a-Service (DFaaS)

A very interesting aspect of the cloud is the possibility to develop and provide forensic-ready systems as utility [66], [109]. Therefore, the term Digital Forensics-as-a-Service (DFaaS) represents a model, in which the cloud service provider is responsible for forensic data collection, or at least is obligated to provide some support [104]. Conceptually, Forensics-by-Design is similar to DFaaS, and proposes a model where the requirements for forensics are integrated into the system development life-cycle [109]. A fair amount of scholars [188]–[190] suggested that these concepts could be a probable solution for the present challenges in IoT and cloud forensics.

H. Big IoT Data Analysis

The rapidly increasing data growth in the IoT domain exceeds the capacity of traditional computing and forensics. Besides processing a tremendous amount of information, it is also the data complexity that could withhold examiners from performing a smooth data analysis. Yaqoob *et al.* [35] underline that the traditional "store-than-process" approach is no longer appropriate for Big IoT forensic data. On the other side, "on-the-fly" data processing will become predominant, and along with the scalability of the analytics algorithms, will shape the IoT Forensics methodology.

I. Usability of Forensics Tools

User Experience is a critical issue in Digital Forensics since every type of misunderstanding could lead to false interpretations and affect real-life cases [191]. Keeping that in mind, Hibshi *et al.* [192] examined the usability aspects of different forensics tools by interviewing forensics professionals about their work. The authors of the study identified considerable usability issues such as: information overload, confusing icons and lack of visualization techniques. According to the survey, the current forensics tools could be improved by implementing consistent and intuitive user interfaces. According to Meffert *et al.* [115], it would be also useful to centralize all tasks in a single Web application, and thereby minimize the use of the terminal.

J. Shutting the IoT Device Down

According to some best-practice guidelines in conventional Digital Forensics science, the evidentiary device must be turned off at the time of confiscation in order to prevent

any alteration of data. However, in the context of modern IoT Forensics, unplugging the system could prevent future access to the evidence data [35], [91]. For that reason, investigators may consider choosing live forensic acquisition methods [193]. Even so, there is a risk that the evidence material will not be accepted in the court if the defence counsel decides to take advantage of the situation and accuse the investigation unit of altering the evidence, deliberately or unknowingly [91].

K. Applying Contemporary Cutting-Edge Research to Forensics

Lilis *at al.* [32] proposed that the field of Digital Forensics could benefit from applying cutting-edge research technologies such as forensic-specialized Information Retrieval (IR) tools. The main contribution of IR techniques to IoT forensic investigations is that after the initial pre-processing, searches could be carried out remarkably fast. One issue in the long-established IR is finding the balance between precision (specificity) and recall (sensitivity), as achieving good results in one of these metrics, usually means worsening the values of the other one. High sensitivity is important for finding all incriminating or exculpatory documents. Thus, recall values are crucial for legal information retrieval, where missing a piece of relevant data could have a serious impact on the investigation outcome [32].

L. Cross-Device Analysis and Data Reduction

Cross-Device and Quick Analysis techniques are not new to the Digital Forensics. First outlined by Garfinkel [194] more than ten years ago, these approaches enable scanning disparate forensic data subsets, and uncover information linkages within a single disk image or across multiple portable devices and cloud stored data. Forensic Feature Extraction (FFE) for example, consists of scanning potential evidence information for certain pseudo-unique identifiers such as email addresses, cookies, SSNs (social security numbers), credit card numbers, etc. By expanding the search to include (seemingly) disparate personal devices and merging data from a variety of sources, forensics professionals can improve the analysis time and gain better understanding of the data corpus [68].

Furthermore, some scholars like Quick and Choo [68] believe that data reduction by selective imaging, coupled with automated data extraction techniques, is the most conceivable way to manage the vast volume of forensic data in a timely manner. A methodology, recently proposed by [68], demonstrates the capability to reduce the volume of the forensic information, while preserving its native source file format and its original metadata. The process aims at facilitating real-time analysis and is specifically designed for large amounts of IoT data [35].

Challenging in the context of expanded Cross-Case and Cross-Device Analysis (CDA) remain the privacy aspects (see Section Privacy and ethical considerations by accessing personal data in Chapter III).

M. Service Level Agreements

The contractual document between the cloud service provider and the cloud customer is called Service Level Agreement (SLA). This document defines the "Terms of use" of the cloud resources. Unfortunately, most of these agreements are non-negotiable and do not incorporate any provisions regarding forensic investigations or evidence recovery [104]. In the future, the Service Level Agreements should include clear information about topics like data access, data acquisition in multi-tenant and multi-jurisdictional environment, confidentiality terms and responsibilities in case of a forensic investigation.

VI. Discussion and Reflexion

The Digital Forensics science is a complex and continuously evolving field. As illustrated in Section V, there are many issues that need further investigation. The aim of this Chapter is, therefore, to cluster and discuss previously identified problems and their possible solutions. Finally, the current section goes one step further by reflecting on the future of the forensics discipline.

A. Forensics Versus Attack Detection

Trends suggest considerable increase in scope, sophistication, and type of cybercrime. The progressing number of victims and economic damage may also be correlated with some novel forms of cybercrime, such as the CaaS model (Crime-as-a-service) which gives inexperienced attackers access to frameworks and tools necessary to carry out a cyber-attack [66].

Another factor contributing to the cybercrime evolution is the evidential discrepancy between attack detection and network forensics. Most of the time, security and forensics practices are treated as completely separated processes, which could result in lag of forensic response and loss of evidence.

A possible solution to this problem may be a hybrid incident detection and forensics model, such as the one proposed by Wang *et al.* [41]. It is designed specifically for M2M networks and consists of two modules: an attack detection module and a forensics analysis module (see Figure 14). The authors pay special attention to the role of honeypots, as well as the role of Intrusion prevention (IPSs) and Intrusion detection systems (IDSs).

Generally, Intrusion detection systems (IDSs) monitor the network traffic and the systems' activities for malicious actions. IPSs are considered extensions of IDSs since they are supposed not to only detect, but also to prevent intrusions. This happens by sending an alarm, dropping malicious packets, resetting the connection or blocking the traffic from the offending IP addresses. Honeypots, on the other hand, are copies of real servers and cover divergent defence methods, such as recording and storing the attacker's behavior.

Wang *et al.* [41] define the following four honeypot modules (see Figure 14): data acquisition module, data storage module, detection module, and implementation module. The detection module, for instance, is responsible for recording the invasion process and redirecting the intrusion data flow to the honeypot

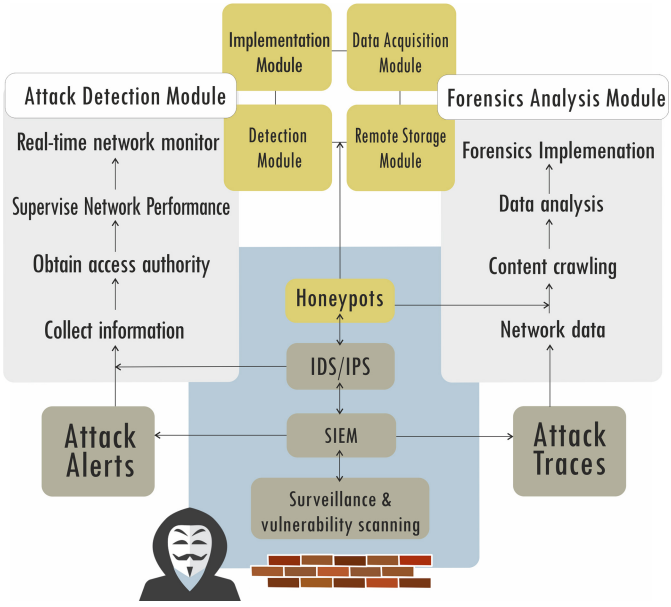

Fig. 14. A hybrid incident detection and forensics model by Wang *et al.* [41].

host, as soon as the IDS detects an attack. However, the most interesting module from a forensics point of view is the remote storage module. It performs a system back up and preserves the original data without any modifications. By doing so, the data storage module guarantees the integrity and the liability of the digital evidence [41].

Honeypots could be a helpful tool in network crime forensics. Nevertheless, they represent a static trap network and become pointless in the exact same moment the attacker is conscious of their presence. Furthermore, the performance and effectiveness of honeypot forensics degrades, due to the huge traffic volume, the heterogeneity of devices, as well as because of some advanced encryption techniques and obfuscation mechanisms (e.g., onion routing) [66].

B. Privacy Risks Mitigation Versus Encryption

Mitigation of privacy risks in the context of RFID-based and IoT Forensics systems, is insufficiently discussed. Of particular concern is the analysis of data stemming from smartphones and smartwatches, since these devices tend to possess a great amount of information on status, activities, preferences and resources, information that extends well beyond the explicit needs of the forensic investigation. Moreover, by analyzing consumption patterns or medical history, one could gain a quite comprehensive view of users' lifestyle, as well as of their physical and mental condition, which could lead to biased assumptions, for example about their internal motivation. Finding the balance between preserving users' privacy and obtaining key evidence will continue to be a major challenge in the field of Digital Forensics. One of the main mechanisms for protecting the right of privacy is the end-to-end data encryption. However, the massive use of per-click encryption tools introduces new challenges for the Digital Forensics, for example, the increasing dependency on the cloud service providers during the process of evidence acquisition.

C. Rise of Anti-Forensics Techniques Versus Achieving Forensics Readiness

The Digital Forensics Readiness (DFR) term represents the capability to *"collect, preserve, protect and analyze Digital Evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or in a Court of law"* [195]. Indeed, it implies that digital forensics approaches should not only be used in post-incident activities, but also to increase the chances of obtaining good results or spending less resources in future investigations [9], [131]. Ergo, DFR could be understood as the *proactive phase* in a cyber investigation (see Figure 5).

As stated in the ISO/IEC 27043 [129], the objectives of implementing DFR practices include:

1) Preserving and improving the level of information security in organizations;
2) Preventing or minimizing interruption of the organization's activities and business processes;
3) Minimizing the cost of conducting a digital forensics investigation;
4) Maximizing the potential value of digital forensics evidence material [196].

Many modern-day organizations have already recognized the need for being forensically ready. Even though it has been acknowledged as a highly recommended objective [62], [196], the integration of Forensics Readiness into IoT systems remains challenging. Kebande *et al.* [196] point out the general lack of IoT architectures that are able to attain such incident preparedness. Thus, the authors propose the DFR-IoT framework [196] that integrates Forensics Readiness guidelines and techniques throughout the whole forensics process, from the initialization until the final reporting phase.

One of the main factors that minimize the potential value of the evidence and, at the same time, double the recourses needed to conduct a forensic investigation, is the rise of anti-forensics techniques. Cybercriminals are aware of the way digital forensics tools work. On that account, they utilize methodologies, known as anti-forensics, which aims at misleading or slowing down the investigators' work [31]. For example, steganographic configurations allow attackers to hide information in metadata (e.g., timestamps) or in unused areas of the hard disk [66]. As the defensive mechanisms become increasingly efficient, even more sophisticated encryption and obfuscation techniques should be expected. In order to deal with the aggressive deployment of anti-forensics methods, researchers and investigators need to come up with improved, proactive and standardized IoT Forensics tools.

D. Multi-Jurisdictional Disputes Versus Collaborative Forensics Knowledge

Modern IoT and cloud technologies are advancing at an extremely fast pace. That is why, law enforcement agencies, legal authorities and governments struggle to address all resulting open legal problems and multi-jurisdictional

disputes [197]. As previously illustrated (see Section Securing Evidence depending on the Deployment and Service model of the Cloud), IaaS and other cloud computing architectures allow data fragmentation and distribution among different countries and continents [109]. Subsequently, it is unclear under which law the case should be prosecuted: the device jurisdiction, the attacker jurisdiction, or the data storage jurisdiction. For that reason, it is necessary to create an international commission, which updates the current legislations and defines uniform procedures in IoT Forensics. This body may also address other issues related to data processing, storage, infrastructure, etc. [104].

Collaboration deficiencies could be found not only on international level, but also between local law enforcement agencies, incident responders and forensic laboratories. Some problems may arise, especially if the forensics investigators have to deal with an IoT device unknown to the practice. In that case, the very first task would require a comprehensive preliminary examination of this particular model. Such a survey is vital to avoid losing evidence as a consequence of a reboot, and includes searching for information in vulnerability databases, user community forums, and academic research [72].

The safe practice imposes accessing the device in read-only mode, as well as using different tools in order to create a working forensic image [66]. As important as it is, finding a way to gain root access to the IoT device is one of the most neglected steps in the forensics process. As already shown in Section Lack of Training and Weak Knowledge Management, first responders tend to turn off the devices found on the crime scene, which could result in deletion of temporary data or encryption of the filesystem [66].

An automated technical solution for bridging this knowledge gap between incident responders and forensic laboratories is described by [73]. The main idea is to "codify" the digital forensics process and make it easily accessible to the police officers at the crime scene via a secure Web-based interface. According to the authors, the Hansken system, developed by the Netherlands Forensics Institute, is a successful example of an automated processing and reporting system for digital traces, available to review remotely during fieldwork. While systems like Hansken may help investigators find signs of deleted or hidden digital evidence, and contribute to timely results, their development is a challenging process due to the constantly evolving forensics standards and computational techniques [73].

E. Tracing the Near-Future Digital Forensics Versus Forensics in the Internet of Everything (IoE)

The functionality of the contemporary IoT devices, as well as their ease of use, is not in question. In combination with cloud computing, IoT applications are increasing the productivity in various fields like manufacturing, supply chains, engineering, commercial use, etc. At the same time, IoT is expected to entail a huge impact on security in all above-mentioned domains. This is why advancements in Digital Forensics need to keep up with the pace of the constantly evolving IoT technology. However, the fast evolution of the field is heavily challenged by the plethora of file formats and OSs, as well as by the extensive use of cryptographic techniques [66]. Newer IoT devices are not supported by the existing forensics tools, making the data extraction process even more challenging. Therefore, advances in Digital Forensics are now more difficult to achieve than in the early years of the discipline.

Another factor contributing to the slow progress in forensics is anonymity. Although anonymization techniques are completely legitimate tools for privacy protection, they are often used by criminals to minimize the risk of being traced [84]. Besides anonymity and rise of encryption techniques, trends suggest a tremendous increase in the amount of generated video content (see Chapter Video-based Evidence Analysis). According to recent YouTube press releases [198], the users of the platform upload more than 500 hours of new video material per minute, which equals to 30,000 hours of new content per hour, or 720,000 hours per day. This means not only an increasing consumers' appetite for video content, but also some new challenges for the near-future forensic investigations that rely on video material.

Furthermore, it should be taken into consideration that the Internet of Things keeps expanding every day. The number of interconnected devices by 2021 is expected to reach 25 billion, producing immense volume of data [199]. Everything that has ever been deployed within the IoT environment may at some point in the future become an object of investigation [29]. In overall, anything and everything in the future will be connected, which will lead to the next evolutionary stage of the Internet of Things, namely the Internet of Everything (IoE).

The Internet of Everything is described as the convergence between data, devices, people and processes [84]. It combines M2M, P2M and P2P communication with the aim to offer broader contextual awareness, and to expand the current service landscape. Therefore, it is also referred to as the Internet of Things and Services (IoT&S). Securing the digital crime scene in the era of the Internet of Everything will be not only problematic, but nearly impossible. While people or physical devices could be easily located, forensically relevant data and processes will continue leaking, even during examination [68]. This will clarify the need for more dynamic forensic practices. Furthermore, the forensics discipline of the future will require privacy-aware collaboration, cross-cutting computational techniques such as AI predictive analytics, run-time verification, and adaptive data collection [76]. The process of data reduction and bulk data analysis will become even more important in the coming years. Digital forensic practitioners will need to take advantage of the supervised and unsupervised learning algorithms, as used in Big Data analytics, in order to cope with the huge amount of data [68]. Finally, to fully understand the challenges of future cybercrime forensics, practitioners and researchers should adopt a multidisciplinary approach [77] and shift their focus from post-event assistance to pre-incident detection strategies and proactive standardization practices.

VII. Concluding Notes

The plethora of challenges in the IoT Forensics reflects the lack of security in cyberspace. Therefore, researchers and forensics professionals work hard to identify tools and solutions that enable the accurate collection and preservation of evidence. Legal authorities, cloud service providers and device manufactures could also contribute to the elimination of IoT security problems. Device manufacturers, for example, should take into consideration that there should be a precise and legal way to extract data from their products, as at some point in the future they might become subjects of an investigation [63]. On the other hand, public institutions and legal authorities should also understand that the IoT Forensics nowadays, is still not in pace with the established discipline of Digital Forensics and therefore, there is a clear need for more research and funding.

The science community has already recognized that we have reached a critical point in the world of forensics [115]. By presenting current challenges and open issues in the field, this paper also acknowledges the importance of adapting and extending traditional forensics tools to the IoT domain, whilst maintaining forensics principles for extracting and preserving legally acceptable evidence [100]. There is also a need for explicit IoT security regulations and generally agreed-upon standards. Research, business and law institutions should join hands, as with the expansion of the IoT development, challenges will continue to grow.

Appendix

List of Used Acronyms

Abbreviation	*Definition*
3DOS	Drone Disrupted Denial of Service
6loWPAN	IPv6 over Low-Power Wireless Personal Area Network
AAV	Autonomous Automated Vehicle
APTs	Advanced Persistent Threats
BAN	Body Area Network
CaaS	Crime-as-a-Service
CCTV	Closed-Circuit Television
CDA	Cross-Device Analysis
CLAHE	Contrast Limited Adaptive Histogram Equalization
CoC	Chain of Custody
CoAP	Constrained Application Protocol
CSP	Cloud Service Provider
DCoC	Digital Chain of Custody
DDoS	Distributed Denial of Service
DF	Digital Forensics
DFaaS	Digital Forensics-as-a-Service
DFR	Digital Forensics Readiness
DNS	Domain Name System
ESE	Electronically Signed Evidence
FaaS	Forensics-as-a-Service
FFE	Forensic Feature Extraction
FRF	Forensically Relevant Files
FIF	Forensically Irrelevant Files
GDPR	General Data Protection Regulation
HPC	High-Performance Computing
IaaS	Infrastructure-as-a-Service
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IR	Information Retrieval
IoT	Internet of Things
IoV	Internet of Vehicles
IVI	In-Vehicle Infotainment
Ipv6	Internet Protocol Version 6
M2M	Machine-to-Machine
MQTT	Message Queuing Telemetry Transport
NFC	Near-Field Communication
P2P	Person-to-Person
P2M	Person-to-Machine
PaaS	Platform-as-a-Service
PDE	Potential Digital Evidence
PPI	Personally Identifiable Information
RFID	Radio-Frequency Identification
RTOS	Real-time Operating System
RHMS	Remote Health Monitoring System
RSU	Roadside Unit
SaaS	Software-as-a-Service
SLA	Service Legal Agreement
TCP	Transmission Control Protocol
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
u-MTC	Ultra-reliable Machine Type Communication
V2CE	Vehicle-to-Consumer Electronics
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-X
VANET	Vehicular Ad-hoc Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VWaaS	Vehicle-Witness-as-a-Service
QoS	Quality of Service
WAN	Wide Area Network.

References

[1] Symantec. (2018). *Internet Security Threat Report (ISTR): Volume 23*. Accessed: Mar. 22, 2019. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[2] S. Alabdulsalam, K. Schaefer, T. Kechadi, and N. A. Le-Khac, "Internet of Things forensics—Challenges and a case study," in *Proc. IFIP Adv. Inf. Commun. Technol.*, vol. 532, 2018, pp. 35–48.

[3] PwC. (2018). *Global Economic Crime and Fraud Survey 2018*. Accessed: Feb. 25, 2019. [Online]. Available: https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf

[4] G. Lally and D. Sgandurra, *Towards a Framework for Testing the Security of IoT Devices Consistently*. Cham, Switzerland: Springer, 2018, pp. 88–102.

[5] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Comput. Sci. Rev.*, vol. 33, pp. 1–48, Aug. 2019.

[6] S. Kunal, A. Saha, and R. Amin, "An overview of cloud-fog computing: Architectures, applications with security challenges," *Security Privacy*, vol. 2, no. 4, pp. 1–14, 2019.

[7] P. Tedeschi and S. Sciancalepore, "Edge and fog computing in critical infrastructures: Analysis, security threats, and research challenges," in *Proc. EuroS&PW*, Jun. 2019, pp. 1–10.

[8] L. Coppolino, S. D'Antonio, G. Mazzeo, and L. Romano, "Cloud security: Emerging threats and current solutions," *Comput. Elect. Eng.*, vol. 59, pp. 126–140, Aug. 2018.

[9] A. Alenezi, N. H. N. Zulkipli, H. F. Atlam, R. J. Walters, and G. B. Wills, "The impact of cloud forensic readiness on security," in *Proc. 7th Int. Conf. Cloud Comput. Services Sci.*, 2017, pp. 539–545.

[10] A. Cook *et al.*, *Internet of Cloud: Security and Privacy Issues*. Cham, Switzerland: Springer, 2018, pp. 271–301.

[11] G. Ramachandra, M. Iftikhar, and F. A. Khan, "A comprehensive survey on security in cloud computing," *Procedia Comput. Sci.*, vol. 110, no. 2012, pp. 465–472, 2017.

[12] M. Hossain, R. Hasan, and A. Skjellum, "Securing the Internet of Things: A meta-study of challenges, approaches, and open problems," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. Workshop (ICDCSW)*, 2017, pp. 220–225.

[13] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open issues," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[14] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Security Appl.*, vol. 38, pp. 8–27, Feb. 2018.

[15] M. Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, "Enforcing security in Internet of Things frameworks: A systematic literature review," *Internet Things*, vol. 6, Jun. 2019, Art. no. 100050.

[16] J. Gubbi, R. Buyya, and S. Marusic, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 1, pp. 1–19, 2013.

[17] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019.

[18] S. Balaji, K. Nathani, and R. Santhakumar, "IoT technology, applications and challenges: A contemporary survey," *Wireless Pers. Commun.*, vol. 108, pp. 363–388, Apr. 2019.

[19] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Comput. Netw.*, vol. 144, pp. 17–39, Oct. 2018.

[20] M. Z. Hasan, H. Al-Rizzo, and F. Al-Turjman, "A survey on multipath routing protocols for QoS assurances in real-time wireless multimedia sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1424–1456, 3rd Quart., 2017.

[21] A. Adeel *et al.*, *A Survey on the Role of Wireless Sensor Networks and IoT in Disaster Management*. Singapore: Springer, 2019, pp. 57–66.

[22] R. Ahmed, A. K. Malviya, M. J. Kaur, and V. P. Mishra, "Comprehensive survey of key technologies enabling 5G-IoT," *SSRN Electron. J.*, Apr. 2019, pp. 488–492.

[23] J. Yin, Z. Yang, H. Cao, T. Liu, Z. Zhou, and C. Wu, "A survey on Bluetooth 5.0 and mesh," *ACM Trans. Sens. Netw.*, vol. 15, no. 3, pp. 1–29, 2019.

[24] M. Bembe, A. Abu-Mahfouz, M. Masonta, and T. Ngqondi, "A survey on low-power wide area networks for IoT applications," *Telecommun. Syst.*, vol. 71, no. 2, pp. 249–274, 2019.

[25] F. Al-Turjman, E. Ever, and H. Zahmatkesh, "Small cells in the forthcoming 5G/IoT: Traffic modelling and deployment overview," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 28–65, Aug. 2019.

[26] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[27] M. Agiwal, N. Saxena, and A. Roy, "Towards connected living: 5G enabled Internet of Things (IoT)," *IETE Tech. Rev.*, vol. 36, no. 2, pp. 190–202, 2019.

[28] H. Ullah, N. G. Nair, A. Moore, C. Nugent, P. Muschamp, and M. Cuevas, "5G communication: An overview of vehicle-to-everything, drones, and healthcare use-cases," *IEEE Access*, vol. 7, pp. 37251–37268, 2019.

[29] 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.

[30] Á. MacDermott, T. Baker, and Q. Shi, "IoT Forensics: Challenges for the Ioa era," in *Proc. 9th IFIP Int. Conf. New Technol. Mobile Security (NTMS)*, Jan. 2018, pp. 1–5.

[31] A. Alenezi, H. F. Atlam, R. Alsagri, M. O. Alassafi, and G. B. Wills, "IoT forensics: A state-of-the-art review, challenges and future directions," in *Proc. 4th Int. Conf. Complexity Future Inf. Syst. Risk (COMPLEXIS)*, May 2019, pp. 106–115.

[32] D. Lillis, B. Becker, T. O'Sullivan, and M. Scanlon, "Current challenges and future research areas for digital forensic investigation," in *Proc. 11th ADFSL Conf. Digit. Forensics Security Law (CDFSL)*, Daytona Beach, FL, USA, May 2016.

[33] M. Y. Arafat, B. Mondal, and S. Rani, "Technical challenges of cloud forensics and suggested solutions," *Int. J. Sci. Eng. Res.*, vol. 8, no. 8, pp. 1142–1149, 2017.

[34] S. Zawoad and R. Hasan, "Digital forensics in the age of big data: Challenges, approaches, and opportunities," in *Proc. IEEE 17th Int. Conf. High Perform. Comput. Commun. IEEE 7th Int. Symp. Cyberspace Safty Security IEEE 12th Int. Conf. Embedded Softw. Syst.*, Aug. 2015, pp. 1320–1325.

[35] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, "Internet of Things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Gener. Comput. Syst.*, vol. 92, pp. 265–275, May 2019.

[36] L. Sadineni, E. Pilli, and R. B. Battula, *A Holistic Forensic Model for the Internet of Things*. Cham, Switzerland: Springer Int., 2019.

[37] M. Hossain, "Towards a holistic framework for secure, privacy-aware, and trustworthy Internet of Things using resource-efficient cryptographic schemes," Ph.D. dissertation, Apr. 2018, doi: 10.13140/RG.2.2.33117.72165.

[38] H. Chung, J. Park, and S. Lee, "Digital forensic approaches for Amazon Alexa ecosystem," in *Proc. 17th Annu. DFRWS USA*, 2017, pp. S15–S25.

[39] M. Al-Sharrah, A. Salman, and I. Ahmad, "Watch your smartwatch," in *Proc. Int. Conf. Comput. Sci. Eng. (ICCSE)*, 2018, pp. 1–5.

[40] C. M. Rondeau, M. A. Temple, and J. Lopez, "Industrial IoT cross-layer forensic investigation," *Wiley Interdiscip. Rev. Forensic Sci.*, vol. 1, no. 1, 2019, Art. no. e1322.

[41] K. Wang, M. Du, Y. Sun, A. Vinel, and Y. Zhang, "Attack detection and distributed forensics in machine-to-machine networks," *IEEE Netw.*, vol. 30, no. 6, pp. 49–55, Nov./Dec. 2016.

[42] A. Tekeoglu and A. Tosun, "Investigating security and privacy of a cloud-based wireless IP camera: NetCam," in *Proc. 24th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Oct. 2015, pp. 1–6.

[43] E. Knight, S. Lord, and B. Arief, "Lock picking in the era of Internet of Things," in *Proc. IEEE CPS Workshop Data Security Privacy Forensics Trust (DSPFT)*, 2019, pp. 835–842.

[44] F. Al-Turjman and M. Abujubbeh, "IoT-enabled smart grid via SM: An overview," *Future Gener. Comput. Syst.*, vol. 96, pp. 579–590, Jul. 2019.

[45] 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 IEEE Green Comput. Commun. IEEE Cyber Phys. Soc. Comput. IEEE Smart Data iThings-GreenCom-CPSCom-SmartData*, Jan. 2018, pp. 274–279.

[46] R. Abassi, "VANET security and forensics: Challenges and opportunities," *Wiley Interdiscip. Rev. Forensics Sci.*, vol. 1, no. 2, 2019, Art. no. e1324.

[47] M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A trustworthy forensic investigation framework for the Internet of Vehicles (IoV)," in *Proc. IEEE 2nd Int. Congr. Internet Things (ICIOT)*, Oct. 2017, pp. 25–32.

[48] E. K. Lee, M. Gerla, G. Pau, U. Lee, and J. H. Lim, "Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs," *Int. J. Distrib. Sens. Netw.*, vol. 12, no. 9, pp. 1–14, 2016.

[49] F. Al-Turjman, J. P. Lemayian, S. Alturjman, and L. Mostarda, "Enhanced deployment strategy for the 5G drone-BS using artificial intelligence," *IEEE Access*, vol. 7, pp. 75999–76008, 2019.

[50] A. Renduchintala, F. Jahan, R. Khanna, and A. Y. Javaid, "A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework," *Digit. Invest.*, vol. 30, pp. 52–72, Sep. 2019.

[51] U. Jain, M. Rogers, and E. T. Matson, "Drone forensic framework: Sensor and data identification and verification," in *Proc. IEEE Sensors Appl. Symp. (SAS)*, 2017, pp. 1–6.

[52] M. A. Ferrag and L. Maglaras, "DeliveryCoin: An IDS and blockchain-based delivery framework for drone-delivered services," *Computers*, vol. 8, no. 3, p. 58, 2019.

[53] N. M. Karie, V. R. Kebande, H. S. Venter, and K.-K. R. Choo, "On the importance of standardising the process of generating digital forensic reports," *Forensics Sci. Int. Rep.*, vol. 1, Apr. 2019, Art. no. 100008.

[54] 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*, Oct. 2013, pp. 608–615.

[55] A. Nieto, R. Rios, and J. Lopez, "IoT-forensics meets privacy: Towards cooperative digital investigations," *Sensors*, vol. 18, no. 2, p. E492, Feb. 2018.

[56] A. Nieto, R. Rios, and J. Lopez, "A methodology for privacy-aware IoT-forensics," in *Proc. 16th IEEE Int. Conf. Trust Security Privacy Comput. Commun. 11th IEEE Int. Conf. Big Data Sci. Eng. 14th IEEE Int. Conf. Embedded Softw. Syst.*, 2017, pp. 626–633.

[57] J. H. Ryu, P. K. Sharma, J. H. Jo, and J. H. Park, "A blockchain-based decentralized efficient investigation framework for IoT digital forensics," *J. Supercomput.*, vol. 75, pp. 4372–4387, Mar. 2019.

[58] A. H. Lone and R. N. Mir, "Forensic-chain: Ethereum blockchain based digital forensics," *Sci. Practice Cyber Security. J.*, vols. 1–2, pp. 21–27, Dec. 2017.

[59] D. P. Joseph and J. Norman, "An analysis of digital forensics in cyber security," in *Proc. Adv. Intell. Syst. Comput.*, vol. 815, 2019, pp. 701–708.

[60] J. Patel, "Forensic investigation life cycle (FILC) using 6 'R'policy for digital evidence collection and legal prosecution," *Int. J. Emerg. Trends Technol.*, vol. 2, no. 1, pp. 129–132, 2013.

[61] J. Cosic and G. Cosic, "Chain of custody and life cycle of digital evidence," *Comput. Technol. Apl.*, vol. 3, pp. 126–129, Aug. 2012.

[62] M. Chernyshev, S. Zeadally, Z. 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 2018.

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

[64] R. C. Joshi and E. S. Pilli, *Computer Communications and Networks Fundamentals of Network Forensics A Research Perspective*. London, U.K.: Springer-Verlag, 2016.

[65] 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.

[66] L. Caviglione, S. Wendzel, and W. Mazurczyk, "The future of digital forensics: Challenges and the road ahead," *IEEE Security Privacy*, vol. 15, no. 6, pp. 12–17, Nov./Dec. 2017.

[67] European Union Agency for Cybersecurity (ENISA). *Major DDoS Attacks Involving IoT Devices*. Accessed: Aug. 25, 2019. [Online]. Available: https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices

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

[69] U.S. Food and Drug Administration. (2019). *Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin Home Transmitter: FDA Safety Communication*. Accessed: Mar. 5, 2019. [Online]. Available: https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm535843.htm

[70] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *Proc. Int. Conf. IoT Soc. Mobile Anal. Cloud (I-SMAC)*, 2017, pp. 32–37.

[71] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 355–373, 2018.

[72] F. Servida and E. Casey, "IoT forensic challenges and opportunities for digital traces," *Digit. Invest.*, vol. 28, pp. S22–S29, Apr. 2019.

[73] E. Casey, "The chequered past and risky future of digital forensics," *Aust. J. Forensics Sci.*, vol. 51, no. 6, pp. 649–664, 2019.

[74] *Discover Key Trends & Insights on Disruptive Technologies & IoT Innovations*, GrowthEnabler, Bengaluru, India, Apr. 2017.

[75] *Industrial IoT (IIoT) Market Size & Forecast to 2026*, Market Study Rep., Selbyville, DE, USA, 2019.

[76] H. Abie, "Cognitive cybersecurity for CPS-IoT enabled healthcare ecosystems," in *Proc. Int. Symp. Med. Inf. Commun. Technol. (ISMICT)*, May 2019, pp. 1–6.

[77] H. Chi, T. Aderibigbe, and B. C. Granville, "A framework for IoT data acquisition and forensics analysis," in *Proc. IEEE Int. Conf. Big Data*, 2019, pp. 5142–5146.

[78] M. S. Obaidat, S. P. Rana, and T. Maitra, *Biometric-Based Physical and Cybersecurity Systems*. Cham, Switzerland: Springer, Oct. 2019.

[79] F. Al-Turjman and A. Malekloo, "Smart parking in IoT-enabled cities: A survey," *Sustain. Cities Soc.*, vol. 49, May 2019, Art. no. 101608.

[80] *The Drone Market Report 2019: Commercial Drone Market Size and Forecast (2019–2024)*, Res. Markets, Dublin, Ireland, 2019.

[81] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of Vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Proc. IEEE World Forum Internet Things Internet*, 2014, pp. 241–246.

[82] *Autonomous Vehicle Sales Forecast 2018*, SupplierInsight, Stamford, CT, USA, 2018.

[83] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 10–21, Feb. 2014.

[84] J. Toldinas, R. Damaševičius, A. Venčkauskas, V. Jusas, and D. H. Grigaliûnas, "Suitability of the digital forensic tools for investigation of cyber crime in the Internet of Things and Services," in *Proc. 3rd Int. Virtual Res. Conf. Technol. Discipl.*, vol. 3, Mar. 2016, pp. 86–97.

[85] M. Gerla, J. T. Weng, and G. Pau, "Pics-on-wheels: Photo surveillance in the vehicular cloud," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, 2013, pp. 1123–1127.

[86] *Smart Home Report 2019*, Statista, Hamburg, Germany, 2019.

[87] *Digital Health Market Share Trends 2019–2025 Growth Forecast Report*, Glob. Market Insights, Pune, India, 2019.

[88] *Forecast: Wearable Electronic Devices, Worldwide*, Gartner Inc., Stamford, CO, USA, 2018.

[89] N. Rana, G. Sansanwal, K. Khatter, and S. Singh, "Taxonomy of digital forensics: Investigation tools and challenges," *arXiv:1709.06529*, Aug. 2017.

[90] NIST. (2014). *Cloud Computing Forensic Science Challenges—Draft NISTIR 8006*. Accessed: Mar. 22, 2019. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf

[91] H. Arshad, A. B. Jantan, and O. I. Abiodun, "Digital forensics: Review of issues in scientific validation of digital evidence," *J. Inf. Process. Syst.*, vol. 14, no. 2, pp. 346–376, 2018.

[92] M. Al Fahdi, N. L. Clarke, and S. M. Furnell, "Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions," in *Proc. Conf. Inf. Security South Africa (ISSA)*, 2013, pp. 1–8.

[93] Y.-Y. Teing, A. Dehghantanha, and K.-K. R. Choo, "CloudMe forensics: A case of big data forensic investigation," *Concurrency Comput.*, vol. 30, no. 5, pp. 1–12, 2018.

[94] 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. Forensics Security (ISDFS)*, 2017, pp. 1–6.

[95] R. C. Hegarty, D. J. Lamb, and A. Attwood, "Digital evidence challenges in the Internet of Things," in *Proc. 10th Int. Netw. Conf. (INC)*, 2014, pp. 163–172.

[96] O. Yakubu, O. Adjei, and N. Babu, "A review of prospects and challenges of Internet of Things," *Int. J. Comput. Appl.*, vol. 139, no. 10, pp. 33–39, 2016.

[97] M. E. Alex and R. Kishore, "Forensics framework for cloud computing," *Comput. Elect. Eng.*, vol. 60, pp. 193–205, May 2017.

[98] D. Quick and K.-K. R. Choo, "Impacts of increasing volume of digital forensic data: A survey and future research challenges," *Digit. Invest.*, vol. 11, no. 4, pp. 273–294, Dec. 2014.

[99] *Merit Medical Endotek—Products*. Accessed: Mar. 2, 2019. [Online]. Available: https://meritsensor.com/products/

[100] E. Oriwoh and G. Williams, "Internet of Things: The argument for smart forensics," in *Handbook of Research on Digital Crime*, vol. 42. Hershey, PA, USA: IGI Glob., 2014, pp. 1–8.

[101] R. Mckemmish, "When is digital evidence forensically sound?" in *Advances in Digital Forensics IV*, vol. 285. New York, NY, USA: Springer, 2008, pp. 3–15.

[102] A. Balogun and S. Zhu, "Privacy impacts of data encryption on the efficiency of digital forensics technology," *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 5, pp. 36–40, 2013.

[103] M. M. Losavio, K. P. 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.

[104] S. O'Shaughnessy and A. Keane, "Impact of cloud computing on digital forensic investigations," in *Proc. IFIP Adv. Inf. Commun. Technol.*, vol. 410, 2013, pp. 291–303.

[105] W. Ejaz and A. Anpalagan, *Blockchain Technology for Security and Privacy in Internet of Things*. Cham, Switzerland: Springer, 2019, pp. 47–55.

[106] D. P. Le, H. Meng, L. Su, S. L. Yeo, and V. Thing, "BIFF: A blockchain-based IoT forensics framework with identity privacy," in *Proc. IEEE Annu. Int. Conf. TENCON*, Oct. 2019, pp. 2372–2377.

[107] S. Brotsis *et al.*, "Blockchain solutions for forensic evidence preservation in IoT environments," in *Proc. NetSoft*, Jun. 2019, pp. 24–28.

[108] R. Verma, J. Govindaraj, and G. Gupta, "DF 2.0: Designing an automated, privacy preserving, and efficient digital forensic framework," in *Proc. Annu. ADFSL Conf. Digit. Forensics Security Law*, 2018, pp. 127–150.

[109] 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, Mar. 2017.

[110] B. Duncan, A. Happe, and A. Bratterud, "Using unikernels to address the cloud forensic problem and help achieve EU GDPR compliance," in *Proc. 9th Int. Conf. Cloud Comput. GRIDs Virtual. Cloud Comput.*, Feb. 2018, pp. 71–76.

[111] *The State Of GDPR Readiness*, Forrester Res., Cambridge, MA, USA, 2018.

[112] *First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities*, EDPB, Brussels, Belgium, 2019.

[113] N. H. N. Zulkipli, A. Alenezi, and G. B. Wills, "IoT forensic: Bridging the challenges in digital forensic and the Internet of Things," in *Proc. IoTBDS*, 2017, pp. 315–324.

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

[115] C. Meffert, D. Clark, I. M. Baggili, and F. Breitinger, "Forensic state acquisition from Internet of Things (FSAIoT)," in *Proc. 12th Int. Conf. Availability Rel. Security (ARES)*, 2017, pp. 1–11.

[116] R. Ahmed and M. L. Ali, "Minimization of security issues in cloud computing," *J. Inf. Commun. Technol. Robot. Appl.*, vol. 3, no. 1, pp. 1–39, 2017.

[117] *Cloud Computing Top Threats in 2016*, Cloud Security Alliance, Singapore, 2016.

[118] *Journey to the Cloud*, KPMG, Amstelveen, The Netherlands, 2016.

[119] *Forecast: Public Cloud Services, Worldwide, 2016–2022*, Gartner, Stamford, CO, USA, 2018.

[120] T. Hou. (2019). *IaaS vs PaaS vs SaaS Enter the Ecommerce Vernacular: What You Need to Know, Examples & More*. Accessed: Oct. 6, 2019. [Online]. Available: https://www.bigcommerce.com/blog/wp-content/uploads/post-pdfs/BigCommerce-saas-vs-paas-vs-iaas.pdf

[121] M. Lang, M. Wiesche, and H. Krcmar, "Criteria for selecting cloud service providers: A Delphi study of quality-of-service attributes," *Inf. Manag.*, vol. 55, no. 6, pp. 746–758, Sep. 2018.

[122] Townsend Security. (2019). *The Definitive Guide to Encryption Key Management Fundamentals*. Accessed: Mar. 16, 2019. [Online]. Available: https://info.townsendsecurity.com/definitive-guide-to-encryption-key-management-fundamentals

[123] Y. R. Stoyanov, "An approach to use the Web services and open source software to store and share user applications and data," in *Proc. Annu. Univ. Sci. Conf. NVU*, vol. 9, 2014, pp. 92–96.

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

[125] O. Adjei, N. C. Babu, and O. Yakubu, "A review of digital forensic challenges in the Internet of Things (IoT)," *Int. J. Mech. Eng. Technol.*, vol. 9, no. 1, pp. 915–923, 2018.

[126] 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.

[127] S. Zawoad, A. K. Dutta, and R. Hasan, "SecLaaS: Secure logging-as-a-service for cloud forensics," in *Proc. AsiaCCS*, Feb. 2013, pp. 219–230.

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

[129] (2015). *ISO/IEC-27043—Information Technology—Security Techniques—Incident Investigation Principles and Processes*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/44407.html

[130] V. R. Kebande *et al.*, "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.

[131] V. R. Kebande and H. S. Venter, "Novel digital forensic readiness technique in the cloud environment," *Aust. J. Forensics Sci.*, vol. 50, no. 5, pp. 552–591, 2018.

[132] V. R. Kebande, N. M. Karie, A. Michael, S. M. G. Malapane, and H. S. Venter, "How an IoT-enabled 'smart refrigerator' can play a clandestine role in perpetuating cyber-crime," in *Proc. IST Africa Week Conf. IST-Africa*, 2017, pp. 1–10.

[133] 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 (ARES)*, 2017, pp. 1–7.

[134] L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, "A digital forensics framework for smart settings," in *Proc. WiSec*, 2019, pp. 332–333.

[135] L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, "IoTDots: A digital forensics framework for smart environments," 2018.

[136] ISO. *ISO/IEC 29100:2011/Amd 1:2018—Information Technology—Security Techniques—Privacy Framework—Amendment 1: Clarifications*. Accessed: Oct. 4, 2019. [Online]. Available: https://www.iso.org/standard/73722.html

[137] H. F. Atlam, G. B. Wills, A. Alenezi, and M. O. Alassafi, "Blockchain with Internet of Things: Benefits, challenges, and future directions," *Int. J. Intell. Syst. Appl.*, vol. 10, no. 6, pp. 40–48, 2018.

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

[139] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," *Inf. Sci.*, vol. 491, pp. 151–165, Jul. 2019.

[140] S. Singh, I. H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology," *Int. J. Distrib. Sens. Netw.*, vol. 15, no. 4, pp. 1–18, 2019.

[141] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for Internet-of-Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, 2017.

[142] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, Oct. 2018.

[143] C. Oham, S. S. Kanhere, R. Jurdak, and S. Jha, "A blockchain based liability attribution framework for autonomous vehicles," *arXiv preprint arXiv:1802.05050*, 2018.

[144] P. Jonsson, S. Carson, A. Torres, K. Ö. P. Lindberg, and A. Karapantelakis, "Ericsson mobility report," p. 28, Jun. 2019.

[145] J. Xiao, S. Li, and Q. Xu, "Video-based evidence analysis and extraction in digital forensic investigation," *IEEE Access*, vol. 7, pp. 55432–55442, 2019.

[146] J. Li, B. Ma, and C. Wang, "Extraction of PRNU noise from partly decoded video," *J. Vis. Commun. Image Represent.*, vol. 57, pp. 183–191, Nov. 2018.

[147] G. Horsman, "Reconstructing streamed video content: A case study on YouTube and Facebook live stream content in the chrome Web browser cache," in *Proc. Digit. Forensics Res. Conf. (DFRWS USA)*, 2018, pp. S30–S37.

[148] M. F. Lohmann, "Liability issues concerning self-driving vehicles," *Eur. J. Risk Regul.*, vol. 7, no. 2, pp. 335–340, 2016.

[149] P. Koopman and M. Wagner, "Autonomous vehicle safety: An interdisciplinary challenge," *IEEE Intell. Transp. Syst. Mag.*, vol. 9, no. 1, pp. 90–96, 2017.

[150] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.

[151] K. M. S. Rahman, M. Bishop, and A. Holt, "Internet of Things mobility forensics," in *Proc. Inf. Security Res. Educ. (INSuRE) Conf. (INSuRECon)*, Sep. 2016, pp. 1–7.

[152] 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.

[153] K. Hammoudi *et al.*, "Developing vision-based and cooperative vehicular embedded systems for enhancing road monitoring services," *Procedia Comput. Sci.*, vol. 52, no. 1, pp. 389–395, 2015.

[154] *Small Unmanned Air System (SUAS) Assessment*, U.K. Airprox Board, London, U.K., 2019.

[155] *Gatwick Airport in Fresh Drone Drama as Flights Are Forced to Divert to Stansted When Device Is Spotted Nearby*, Telegraph, West Bengal, India, 2019.

[156] F. E. Salamh, U. Karabiyik, M. K. Rogers, and F. Al-Hazemi, "Drone disrupted denial of service attack (3DOS): Towards an incident response and forensic analysis of remotely piloted aerial systems (RPASs)," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf.*, 2019, pp. 704–710.

[157] SWGDE. *Scientific Working Group on Digital Evidence*. Accessed: Mar. 4, 2019. [Online]. Available: https://www.swgde.org/

[158] E. Leverett, R. Clayton, and R. Anderson, "Standardisation and certification of safety, security and privacy in the 'Internet of Things,'" JRC Rep., 2017, doi: 10.2760/47559.

[159] *ISO/IEC 27035–1:2016—Information Technology—Security Techniques—Information Security Incident Management—Part 1: Principles of Incident Management*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/60803.html

[160] *ISO/IEC WD 27035-1—Information Technology—Security Techniques—Information Security Incident Management—Part 1: Principles of Incident Management*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/78973.html

[161] *ISO/IEC 27035-2:2016—Information Technology—Security Techniques—Information Security Incident Management—Part 2: Guidelines to Plan and Prepare for Incident Response*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/62071.html

[162] *ISO/IEC WD 27035-2—Information Technology—Security Techniques—Information Security Incident Management—Part 2: Guidelines to Plan and Prepare for Incident Management*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/78974.html

[163] (2014). *ISO/IEC 27037:2012—Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/44381.html

[164] (2005). *ISO/IEC 27001:2005 Information Technology—Security Techniques—Specification for an Information Security Management System*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/44382.html

[165] (2015). *ISO/IEC 27040:2015(E)—Information Technology—Security Techniques—Storage Security*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/44404.html

[166] (2014). *ISO/IEC 27041—Guidance on Assuring Suitability and Adequacy of Incident Investigative Methods*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/44405.html

[167] *ISO/IEC 27042:2015—Information Technology—Security Techniques—Guidelines for the Analysis and Interpretation of Digital Evidence*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/44406.html

[168] *ISO/IEC 27050-1:2016—Information Technology—Security Techniques—Electronic Discovery—Part 1: Overview and Concepts*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/63081.html

[169] *ISO/IEC FDIS 27050-1—Information Technology—Electronic Discovery—Part 1: Overview and Concepts*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/78647.html

[170] *ISO/IEC 30121:2015—Information Technology—Governance of Digital Forensic Risk Framework*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/53241.html

[171] *ISO/IEC 27017:2015—Information Technology—Security Techniques—Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services*. Accessed: Sep. 25, 2019. [Online]. Available: https://www.iso.org/standard/43757.html

[172] *ISO/IEC 27018:2019—Information Technology—Security Techniques—Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors*. Accessed: Sep. 25, 2019. [Online]. Available: https://www.iso.org/standard/76559.html

[173] (2014). *ISO/IEC 27031:2011 BSI—Information Technology—Security Techniques—Guidelines for Information and Communication Technology Readiness for Business Continuity*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/44374.html

[174] *ISO/IEC WD 27031—Information Technology—Guidelines for ICT Readiness for Business Continuity*. Accessed: Aug. 28, 2019. [Online]. Available: https://www.iso.org/standard/78771.html

[175] *ISO/IEC WD 27030—Information Technology—Security Techniques—Guidelines for Security and Privacy in Internet of Things (IoT) Title Missing*. Accessed: Sep. 25, 2019. [Online]. Available: https://www.iso.org/standard/44373.html

[176] *ISO/IEC 20546:2019—Information Technology—Big Data—Overview and Vocabulary*. Accessed: Sep. 1, 2019. [Online]. Available: https://www.iso.org/standard/68305.html

[177] A. Krivchenkov, B. Misnevs, and D. Pavlyuk, *Intelligent Methods in Digital Forensics: State of the Art*, vol. 1. Cham, Switzerland: Springer Int., 2019.

[178] *ISO 22320:2018—Security and Resilience—Emergency Management—Guidelines for Incident Management*. Accessed: Sep. 25, 2019. [Online]. Available: https://www.iso.org/standard/67851.html

[179] N. D. W. Cahyani, B. Martini, K.-K. R. Choo, and H. Ashman, "An approach to enhance understanding of digital forensics technical terms in the presentation phase of a digital investigation using multimedia presentations," in *Proc. Inst. Comput. Sci. Soc. Informat. Telecommun. Eng.*, 2018, pp. 448–506.

[180] A. Chapman, "Intruder detection through pattern matching and provenance driven data recovery," in *Proc. Cloud Comput.*, Feb. 2018, pp. 58–64.

[181] *Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview*, Ponemon Inst., Traverse City, MI, USA, Jun. 2017, pp. 1–35.

[182] Y. Zhao and B. Duncan, "Could block chain technology help resolve the cloud forensic problem?" in *Proc. 9th Int. Conf. Cloud Comput. GRIDs Virtual. Cloud Comput.*, Feb. 2018, pp. 39–44.

[183] M. Serenhov, "Forensic breach response in compliance with GDPR," M.S. thesis, Dept. Elect. Inf. Technol., Faculty Eng., Lund Univ., Lund, Sweden, 2018.

[184] E. A. Vincze, "Challenges in digital forensics," *Police Pract. Res.*, vol. 17, no. 2, pp. 183–194, 2016.

[185] S. Garfinkel, "Lessons learned writing digital forensics tools and managing a 30TB digital evidence corpus," in *Proc. Digit. Forensics Res. Conf. (DFRWS USA)*, 2012, pp. S80–S89.

[186] A. Shalaginov and K. Franke, *Big Data Analytics by Automated Generation of Fuzzy Rules for Network Forensics Readiness*, vol. 52. Amsterdam, The Netherlands: Elsevier, 2017.

[187] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.

[188] X. Du, N.-A. Le-Khac, and M. Scanlon, "Evaluation of digital forensic process models with respect to digital forensics as a service," in *Proc. 16th Eur. Conf. Cyber Warfare Security (ECCWS)*, 2017, pp. 573–581.

[189] Y. Wen, X. Man, K. Le, and W. Shi, "Forensics-as-a-service (FaaS): Computer forensic workflow management and processing using cloud," in *Proc. Cloud Comput.*, 2013, pp. 208–214.

[190] A. Srinivasan and F. Ferrese, "Forensics-as-a-service (FaaS) in the state-of-the-art cloud," in *Proc. Security Privacy Digit. Forensics Cloud*, 2019, pp. 321–337.

[191] D. R. Kamble and N. Jain, "Digital forensic tools: A comparative approach," *Int. J. Adv. Res. Sci. Eng.*, vol. 4, no. 4, pp. 157–168, 2015.

[192] H. Hibshi, T. Vidas, and L. Cranor, "Usability of forensics tools: A user study," in *Proc. 6th Int. Conf. IT Security Incident Manag. IT Forensics (IMF)*, 2011, pp. 81–91.

[193] P. H. Rughani, "IoT evidence acquisition—Issues and challenges," *Res. India Publ.*, vol. 10, no. 5, pp. 1285–1293, 2017.

[194] S. L. Garfinkel, "Forensic feature extraction and cross-drive analysis," *Digit. Invest.*, vol. 3, pp. 71–81, Sep. 2006.

[195] (2015). *National Technical Authority for Information Assurance, "Good Practice Forensics Readiness Guideline*." Accessed: Jul. 14, 2018. [Online]. Available: https://westessexccg.nhs.uk/about-us/library/policies-1/2278-west-essex-ccg-forensic-readiness-policy/file%0A http://extranet.fylde.gov.uk/assets/files/65/Microsoft-Word-Forensic-Readiness-Policy-2013.pdf

[196] V. R. Kebande, N. M. Karie, and H. S. Venter, "Adding digital forensic readiness as a security component to the IoT domain," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 1, p. 1, 2018.

[197] M. James and P. Szewczyk, "Jurisdictional issues in cloud forensics," in *Proc. 11th Int. Symp. Human Aspects Inf. Security Assurance (HAISA)*, 2017, pp. 225–235.

[198] *YouTube: Hours of Video Uploaded Every Minute 2019—Statista*, Statista, Hamburg, Germany, 2019.

[199] *Top 10 Strategic IoT Technologies and Trends*, Gartner, Stamford, CO, USA, 2018.

[200] S. Blanchard. *Brexit, GDPR and Data Protection: What Happens If the U.K. Becomes a Third Country—Data Protection Network*. Accessed: Oct. 12, 2019. [Online]. Available: https://www.dpnetwork.org.uk/brexit-gdpr-data-protection-uk/

[201] National Research Council Committee on Identifying the Needs of the Forensic Sciences Community. (2015). *Forensics Science International*. Accessed: Mar. 7, 2019. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27043:ed-1:v1:en