Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges

Ibrar Yaqoob[a], Ibrahim Abaker Targio Hashem[b], Arif Ahmed[c], S. M. Ahsan Kazmi[a], Choong Seon Hong[1a]

[a]*Department of Computer Science and Engineering, Kyung Hee University, Yongin 446-701, Korea.*
[b]*School of Computing and IT, Taylor's University, Subang Jaya, Malaysia.*
[c]*Department of Computer Science Engineering, National Institute of Technology, Silchar, India.*

Abstract

The explosive growth of smart objects and their dependency on wireless technologies for communication increases the vulnerability of Internet of Things (IoT) to cyberattacks. Cyberattacks faced by IoT present daunting challenges to digital forensic experts. Researchers adopt various forensic techniques to investigate such attacks. These techniques aim to track internal and external attacks by emphasizing on communication mechanisms and IoT's architectural vulnerabilities. In this study, we explore IoT's novel factors affecting traditional computer forensics. We investigate recent studies on IoT forensics by analyzing their strengths and weaknesses. We categorize and classify the literature by devising a taxonomy based on forensics phases, enablers, networks, sources of evidence, investigation modes, forensics models, forensics layers, forensics tools, and forensics data processing. We also enumerate a few prominent use cases of IoT forensics and present the key requirements for enabling IoT forensics. Finally, we identify and discuss several indispensable open research challenges as future research directions.

Keywords: Internet of Things, Cybersecurity, Internet of Things Forensics, Security, Cybercrime, Smart City

[1]Corresponding author.

1. Introduction

The unprecedented proliferation of miniaturized Internet of Things (IoT) devices, such as smartphones, washing machines, and medical implants, has empowered people to share information with one another [1, 2]. These devices can communicate with one another directly or via Application Programming Interface (API) over the Internet, and they can be controlled by "learned" devices with high computing capabilities, such as cloud servers, that augment smartness to low-computing devices [3–5]. The smartness and communication capabilities of IoT devices offer many beneficial applications to common people, companies, industry, and governments. IoT application is also extended in the areas of transportation, healthcare, and smart cities [6]. In addition, the market trend of IoT is increasing, as indicated by CISCO's estimation of IoT revenue, which will be around $14.4 trillion between 2013 and 2022[2]. However, emerging IoT technologies face various security attacks and threats [7]. Notable threats include virus attacks, mass surveillance, and Denial of Service (DoS) attacks, and disruption of IoT networks [8–10]. To investigate these attacks, well-trained teams must conduct digital investigation, known as IoT forensics, on the crime scene [11–13]. An illustration of security concerns in IoT-based smart environments is provided in Figure 1. **The sources of evidence in IoT forensics include home appliances, cars, medical implants, sensor nodes, and tag readers, among others. In traditional forensics, the sources of evidence can be computers, mobile phones, servers, or gateways [14]. Regarding types of evidence data, IoT data can be available in any vendor-specific format, unlike in traditional forensics wherein data is mostly available in an electronic document or standard file formats [14].**

IoT forensics involves many challenges due to the nonsuitability of currently available digital forensics tools and standard forensics methodologies in the IoT environment [15–18]. IoT devices also generate huge amount of various data that puzzle investigators when deciding the relevant source of evidence and identifying the exact amount of data to be used for further investigation [19].

Several surveys [20–27] were conducted previously on the usage of digital

[2] Accessed on: 17th May 2018 https://www.ironpaper.com/webintel/articles/internet-of-things-market-statistics/

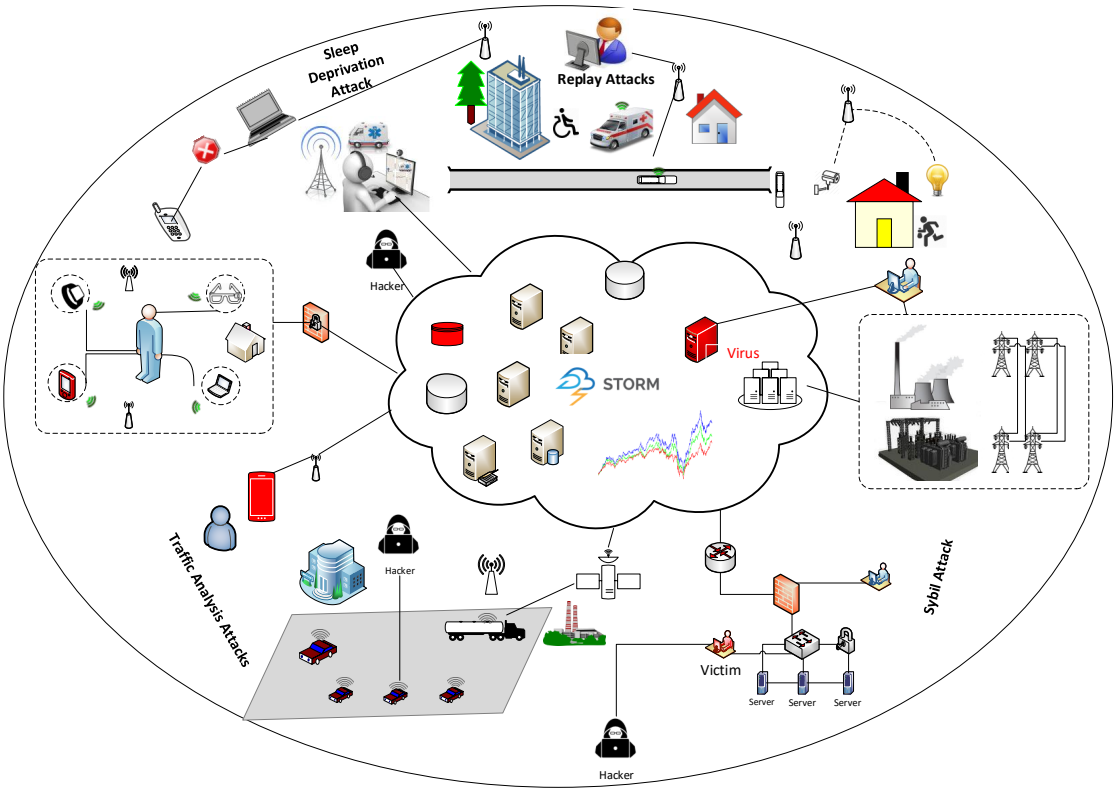

Figure 1: An illustration of security concerns in IoT-based smart environments

forensics in multiple domains, i.e., cloud computing, edge computing, mobile cloud computing, software-defined networks, wireless networks, smart cities, and smart transportation systems, among others. However, none of these surveys comprehensively focused on IoT forensics. In addition, several other important aspects of IoT forensics, which are discussed in the current study, have not been previously reported.

The contributions of this study are as follows:

- We explore IoT's novel factors affecting traditional computer forensics.
- We investigate the state-of-the-art research on IoT forensics.
- We categorize and classify the literature by devising a taxonomy.

- We enumerate a few notable use cases related to IoT forensics.
- We outline and highlight the key requirements for enabling IoT forensics.
- Finally, we identify and discuss several indispensable open research challenges.

The remainder of this paper is organized as follows. We explain IoT's novel factors affecting forensics and investigate the recent literature on IoT forensics in Sections 2–3. We discuss the devised taxonomy in Section 4, whereas we identify and present the possible use cases of IoT forensics in Section 5. Then, we outline and enumerate the key requirements for enabling IoT forensics in Section 6, followed by a discussion on several research challenges to be addressed in the IoT forensics paradigm in Section 7. Finally, we conclude the study in Section 8.

2. Novel factors of IoT affecting forensics

Numerous new factors of IoT affecting traditional computer forensics are outlined in Figure 2. A huge number of diverse and resource-constrained devices are involved in IoT-enabled environments, which generate an enormous amount of data called "Big IoT Data" [28]. A large amount of IoT data prevent the forensics investigator to collect and extract the evidence data smoothly. The main challenges posed by Big IoT Data for the forensics investigators are diverse data formats and lack of real-time log analysis solutions. Digital evidence is one of the fundamental requirements for enabling IoT forensics. Such an evidence can only be obtained by extracting firmware data or acquiring a flash-memory image. In terms of digital evidence, limited visibility and short survival period of the evidences are the new challenges posed by the IoT devices which affect the traditional computer forensic solutions to be applied in the IoT systems. In the smart environments, data are mostly stored and processed on the cloud. In most cases, acquiring access to data for investigation purposes becomes difficult for IoT forensics investigators due to service

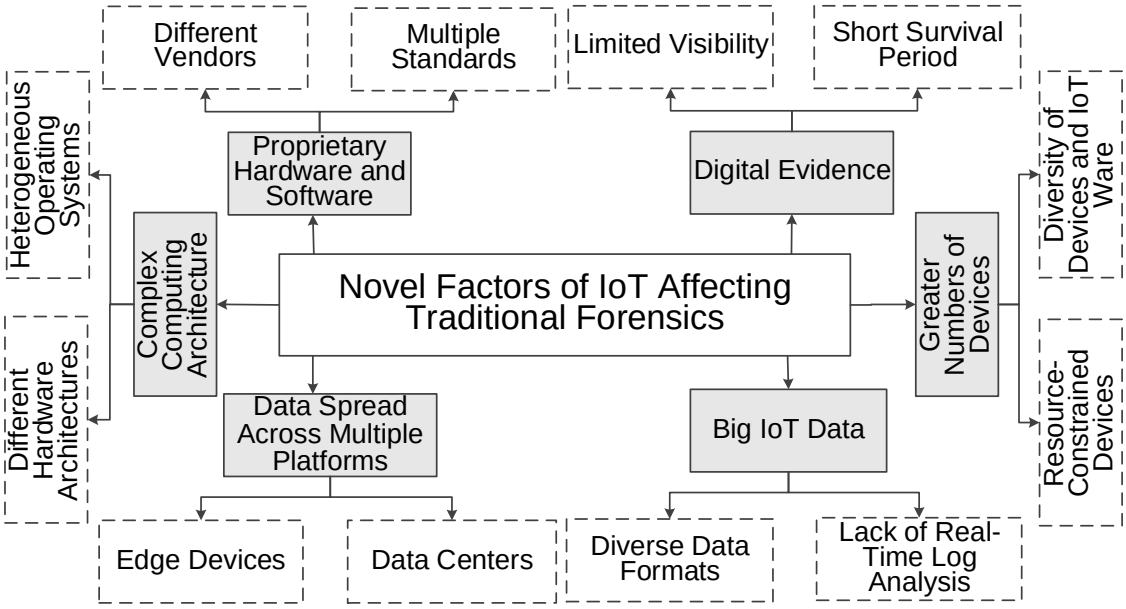

Figure 2: Novel factors of IoT affecting traditional computer forensics

level agreement constraints. In addition, the data of IoT environment are spread across multiple platforms, e.g., on the edge devices and data centers [29, 30]. The computation is also performed mainly at the edge of users' networks, and metadata are transferred to the cloud. In such a scenario, the data are stored in two hierarchies, which create difficulties for forensics investigators in terms of data collection and log data analysis. The two other IoT factors affecting forensics are complex computing architecture (i.e., different hardware architectures and heterogeneous operating systems) and proprietary hardware and software (i.e., different vendors and multiple standards).

3. Recent advances

Although many studies [31–40] are conducted on IoT security, the literature on IoT forensics is scarce. Figure 3 shows the titles of published works on IoT forensics.

Figure 3: Word frequency occurrences in most publications

3.1. Smart home forensics

Smart home devices were the focus of [41], and these devices aim to obtain compromising information. During a crime investigation, smart home devices can play important roles through their motion detectors or microphones. These devices can help in conclusively proving a suspect's location. Three forensic adversaries were constructed, e.g., passive, active, and single-malicious active adversaries. The authors explored two smart home devices, namely, smart light and smart bulb, as case studies. **The findings revealed that enormous amount of data are available to even the passive adversary, which can lead to determining the actions performed at a specific interval of time. However, this work remains in its infancy, and the solution must be automated in the future.**

Forensics Edge Management System (FEMS) was designed and proposed in [42], and this system aims to provide security and forensics services for smart homes. FEMS comprises different functions, namely, network monitoring, intrusion detection and prevention, data logging, and threshold estimation. **FEMS offers numerous benefits, such as automatic detection, intelligence, and flexibility. However, its implementation involves many complexities, and its rigorous testing is taxing.**

According to the authors in [43], security concerns increase as voluminous amount of devices connect to the Internet due to the vulnerabilities of smart devices. Digital forensics techniques are required to cope with such security challenges. Therefore, the authors discussed the need for digital forensics models and methodologies in the IoT paradigm (smart home). The study aimed to make arguments for the importance of smart forensics in cyber-physical environments and smart homes, as in the case of IoT. **Although the authors focused mainly on the applicability of existing forensics techniques in IoT, the existing forensics techniques cannot be fully applied in IoT because of new IoT challenges, such as multiple network involvement.**

In the foreseeable future, the smart home environments will become very common. In this context, a seven-phase forensic investigation framework was proposed, which can help to perform a smooth investigation in the smart home environments [44]. In the framework, phase 1 ensures that a forensics expert is available with an appropriate skills set (e.g., www.openhab.org, www.home-assistant.io). The second phase 2 ensures that all the information used in the smart home are extracted and stored safely. The next phase helps in preserving all the pieces of evidence. A global picture of the system (network topology) is created in phase 4. All the security checks are validated in phase 5. The next phase helps to locate and acquire evidential data. In the last phase, the investigator seeks to make sense of the acquired data. The applicability of the framework has been shown by presenting three case studies. The finding of the study revealed that the proposed framework can facilitate in terms of trustworthy ev-

idence collection and preservation. However, the framework still requires to be validated using the real-world home automation systems.

3.2. Forensics analysis for smart vehicles

The Internet of Vehicles (IoV) systems enable the information sharing between the vehicles and their surrounding sensors. Although the IoV systems have brought numerous opportunities in terms of road safety and traffic management, they brought many new challenges related to the digital forensics. To address the forensics related challenges, the study [45] has proposed a trustworthy investigation framework called Trust-IoV for the Internet of Vehicles systems. The framework helps to collect and preserve the trustworthy evidence from the highly distributed smart vehicles based environment. Furthermore, the framework helps in maintaining a secure provenance of the evidence which leads to ensuring the integrity of the stored evidence. The results of the framework suggested that the framework can operate with minimal overhead in a strong adversarial scenario. The authors in [46] investigated and analyzed the threats to smart vehicles in a smart city. A forensic model was proposed for investigating smart vehicles. Its effectiveness was affirmed by the results. **However, the proposed model is in its infancy, and still requires to be validated using the data traffic generated by the smart vehicles in a real scenario.**

3.3. Forensics analysis for smartphones

In the modern age of technology, people are increasingly relying on smartphones instead of desktop computers for exchanging messages, sharing videos and audios messages. A criminal can exploit the smartphone by performing a number of activities including committing a fraud over e-mail, harassment via text messages, drug trafficking, child pornography, communications related to narcotics, etc [47]. In case of exploitation, it has become very challenging to extract such information from the smartphones for the forensics purposes. To address

this challenge, a study [47] is conducted which helps to perform forensic analysis for the smartphones using Universal Forensic Extraction Device (UFED) physical analyzer. The study has focused on gaining the root access and acquiring data from the Samsung Galaxy S3 phone. The purpose was to provide a vision that forensics analysis can be performed for the smartphones, however, the work was not conclusive.

Transplantation of the recent mobile phones has become a complex task involving the risk of PoP components' destruction. As such, a new solution called "PoP chip-off/TCA Technique" was proposed in [48]. The proposed technique allows the desoldering of PoP components without causing damage and ensures successful transplantation of the latest mobile phones. A new method was also developed and successfully applied to the forensic transplantation of a cryptographic Black-Berry 9900 PGP mobile phone.

3.4. Forensics analysis for drones

A methodology that enables forensic analysis for drones was proposed in [49]. The forensic analysis was performed on DJI Phantom III drone. The study also proposed an open source tool called DRone Open Source Parser (DROP). The tool parses proprietary DAT files extracted from the drone's internal storage. These DAT files are encrypted and encoded. The work also shared preliminary findings on TXT files, which were also proprietary, encrypted, and encoded files found on the mobile device controlling the drone. The TXT files help search important information, such as GPS locations, battery, and flight time, which can be used in forensic analysis later on. **Although the work helps in enabling forensic analysis in drones, it focuses only on the DJI Phantom III. Further work must be done on various types of drones, such as Phantom IV. In addition, the file structures of DAT and TXT must be demystified.**

3.5. Forensics analysis for newer BitTorrent Sync peer-to-peer cloud storage

A methodology was outlined in [50], and this methodology helps in collecting and analyzing the data derived from the newer BitTorrent

Sync peer-to-peer cloud storage service, which acts as a backbone for IoT networks. The experiments were performed using mobile phones, Windows-run computer systems, Mac OS, Ubuntu, iOS, and Android devices. The results revealed that artifacts relating to log-in, log-off, installation, uninstallation, and cloud synchronization metadata are recoverable. Such artifacts are considered important sources of IoT forensics. In addition, the work suggested that the memory snapshot should be obtained as quickly as possible because it increases the likelihood of preserving the artifacts. **This study has many advantages, i.e., the proposed methodology can help in investigating other BitTorrent-Sync-enabled clients sharing similar datasets. However, the proposed methodology was not validated with the original equipment manufacturer.**

3.6. Forensics Analysis for the General IoT Systems

A real-world investigation model for the future heterogeneous IoT systems was proposed in [51]. A threat assessment scenario was developed based on STRIDE and DREAD models. These models revealed that cyber attacks in the IoT systems can lead to serious consequences like death. Moreover, the study found that the existing solutions for the IoT systems do not include security by default, thus posing high risks. A study was conducted [52] to show the impact of the sync data on evidence. Sync data can enable impartial analysis of electronic evidence. In [53], the authors surveyed state-of-the-art in-memory forensic techniques. They explained and highlighted the important changes in designing operating systems in the future. **The authors in [54] has introduced a data reduction and semi-automated investigation process, which helps in scanning the large amount of IoT data. The process helps in enabling real-time analysis of a wide range of IoT data.**

The authors in [55] introduced the concept of acquiring, storing, and transmitting digital evidence reliably and securely to an authorized entity. Certain technologies that can help implement this concept in an IoT environment were discussed as well. In addition, the building blocks of the digital witness were defined. In [56], the authors proposed a new integrative approach that combines cloud-native and cloud-centric forensic for the Amazon Alexa ecosystem.

A forensic investigation framework called "Probe-IoT" was proposed in [57]. The framework helps to find criminal facts in IoT-based systems using the digital ledger, which maintains a track record of all the transactions taking place between IoT devices, users, and cloud services. The theoretical results of the framework reveal that the proposed framework ensures the integrity, confidentiality, and non-repudiation of the evidence. However, the framework has not been evaluated experimentally, and resource efficiency of the framework in terms of computation and storage cast was not analyzed. Another study[58] has proposed a traffic analysis tool, which helps to identify the attacks in IPv6 based low power wireless personal area networks. One of the prime advantages of the tool is that it presents the analysis results in a human-readable format. However, the efficiency of the tool still needs to be improved.

A new IoT forensics model called PRoFIT was proposed in [59]. This model ensures privacy (ISO/IEC 29100:2011) standard during forensic investigations. Ensuring the privacy aims to encourage IoT devices to voluntarily participate in digital forensic investigations. The proposed model was evaluated in actual malware propagation in an IoT-enabled coffee shop.

E. Oriwoh et al. [60] proposed the application of 1-2-3 zone approach to IoT-related digital forensics investigations. Persons related to the crime and possible evidence are identified in Zone 1, whereas all the devices closer to the border of the network reside in Zone 2. All devices outside the network are covered in Zone 3. In this work, the authors also introduced the next-best-thing triage model and combined it with 1-2-3 zone approach when necessary. **The proposed work can provide many benefits such as effective and efficient IoT-related investigation in terms of identifying relevant evidence. However, developing and testing this work are challenging.**

The researchers in [61] proposed a complete tamper-proofing framework based on three-layer architecture. The three layers are physical security mechanisms, encryption, and live forensics protection techniques. **This framework provides many advantages, such as manipulation prevention, software-based protection, and infrequent verification triggering . The only disadvantage of the framework**

is the lack of lightweight features as most of IoT devices have limited resources in terms of battery and processing power.

The authors in [62] aimed to design the best approach in producing a novel model that enables forensics experts to conduct IoT investigations. The authors designed an integrated model based on triage and 1-2-3 zone models for volatile-based data preservation. This study was an extension of other works as it rigorously tested previous forensics investigation approaches. **The proposed approach can help forensics experts conduct IoT investigations with large size-based perspective. However, the automation of this model seems rather difficult in a practical environment.**

In [63], the authors introduced a new definition of IoT forensics. They also systematically analyzed IoT domain to uncover the challenges and issues in the area of digital forensics. A new approach, called Forensic-Aware IoT (FAIoT), was proposed to support the reliability of and bring about new insights into forensic investigations in IoT environment. **However, such an approach was not tested for executing digital forensics in the IoT infrastructure, which might lessen its applicability to practice.**

The researchers in [64] examined the current challenges contributing to the backlog in digital forensics from a technical perspective, which can hamper the discovery of pertinent information for digital investigators. The author also highlighted a number of future research topics that could greatly contribute to a more efficient digital forensic process. As such, combined the negative effect of the challenges can be significantly amplified based on the future research works that include, information retrieval, FPGA processing, and parallelization.

A. Bijalwan et al. [65] addressed the flooding attacks against available resources in IoT environment, where the attack mode increases the difficulty of the investigation. The hackers use random-UDP flooding attacks by sending multiple UDP datagrams of different sizes at a time. This action may result in denial of services to the system and the resources. Thus, the authors proposed a new approach for the forensics investigation of random-UDP flooding attacks. This approach can identify the sources of random-UDP flooding attacks. **However, this proposed solution may be unable to identify real-time attacks**

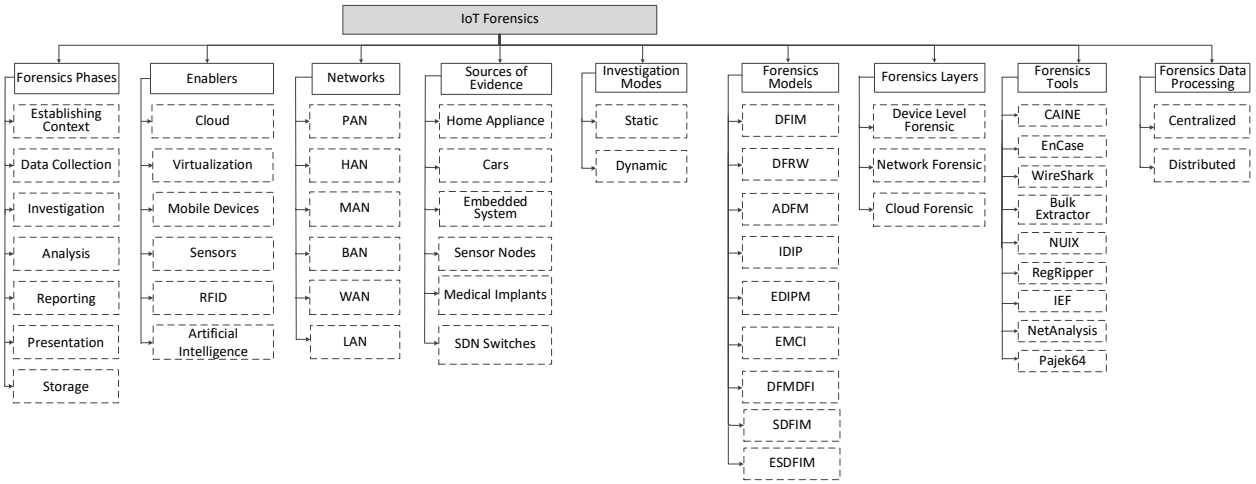

Figure 4: Taxonomy of IoT Forensics

generated by zero-day attacks.

4. Taxonomy of IoT forensics

This section describes the taxonomy of IoT forensics illustrated in Figure 4. The attributes of this taxonomy include forensics phases, enablers, networks, sources of evidence, investigation modes, forensics models, forensics layers, forensics tools, and forensics data processing. Herein, these attributes are briefly discussed.

4.1. Forensics phases

A typical IoT forensics investigation starts with establishing context. The investigation team applies many security measurements, such software and security tools, on the vast data to be collected from different locations [66]. The law enforcement related to the investigation, such as privacy, copyright, and information technology law, among others, are thoroughly reaffirmed and agreed by the investigator before the actual investigation. Evidence is then collected from various sources of evidence. It investigated and analyzed further in the next phase. Based on the evidence, the final conclusion is reported in the document and

presented to the relevant parties. At the final phase, the collected data and the final reports are archived in a digital form for future use.

4.2. Enablers

IoT is composed of various technologies, such as sensor nodes, mobile devices, virtualization, cloud, Radio Frequency Identification (RFID), network equipment, and Artificial Intelligence (AI). These technologies play individual roles during the forensics investigation process. Core IoT devices, such as sensor nodes and mobile devices, are used to collect evidence from the crime scene after the attack. Cloud and virtualization technology provide on-demand, scalable, elastic, compute-as-a-service support during the whole forensics process. RFID is used extensively in sensor devices for object identification. Network equipment, such as routers, switches, and Software Defined Networking (SDN) switches, enable to track packet tracing. AI techniques are used extensively in analyzing the data collected.

4.3. Networks

Network attributes refer to the type of network connected to IoT devices in the crime scene. Network type plays a great role during the investigation process, and it ensures that the area of the region is covered and law enforcement is obeyed. Local area network (LAN), Metropolitan Area Network (MAN), and Personal Area Network (PAN) are extensively used for interconnecting IoT devices within a small range. Examples of these networks are surveillance cameras installed in street and shopping malls. Home appliances, such as washing machines and refrigerators, are connected to the Home Area Network (HAN). Cloud computing plays a great role for IoT devices in terms of data storage and processing. IoT appliances are connected to the WAN network to integrate the cloud application through API.

4.4. Sources of evidence

Crime-related information in IoT can be collected from the different crime scenes focusing on the core source of evidence [67]. In IoT, the data can reside predominantly in the devices, such as home appliances, sensor nodes, medical implants, embedded systems, and cars. Although

the memory spaces of IoT applications are low, valuable information is sent to the central processing computer for processing through the network. Data, such as the system log and temporary cache memory, can be used as sources of evidence. These data can be retrieved by tracing many network devices, such as routers, SDN, and switches, among others.

4.5. Investigation modes

Investigation mode categorizes the type of investigation based on the timeline of the investigation. Static mode is the traditional investigation method performed after identifying the attack in the IoT system. As a result of the attack, IoT data are already corrupted or deleted. Static mode recovers data using universal serial bus and scanning cache memory, among others. IoT forensics investigation sometimes requires the system to be alive during the process to discover fresh data, such as open network connection, memory dumps, and running processes, for extracting important sources of evidence. This type of investigation mode is known as dynamic mode.

4.6. Forensics models

The forensics investigations for IoT applications are conducted within standard models so that the relevant evidence collected are acceptable to the court [68]. All the existing standard models follow basic phases of forensics investigation, i.e., establishing context, data collection, investigation, analysis, and reporting, among others. Digital Forensics Investigation Model (DFIM) is a four-phase model that primarily aims to uncover hidden evidence in the collected data. However, it is not concerned on actual evidence, i.e., physical evidence, which is unfavorable in IoT's case. **Other existing forensic models include Digital Forensic Research Workshop (DFRW), Abstract Digital Forensic Model (ADFM), Integrated Digital Investigation Model (IDIP), Enhanced Digital Investigation Process Model (EDIPM), Extended Model of Cybercrime Investigation (EMCI), Digital Forensic Model for Digital Forensic Investigation (DFMDFI), Systematic Digital Forensic Investigation Model (SDFIM), and Enhanced Systematic Digital Forensic Investigation Model (ESDFIM) [69]. DFRW is**

based on seven phases (e.g., identification, preservation, collection, examination, analysis, presentation, and decision). ADFM has added three new components (e.g., preparation, approach strategy, and return of evidence), which were missing in DFRW. IDIP is a five-phase model (e.g., readiness, deployment, physical crime scene investigation, digital crime scene investigation, and review). EDIPM aims to enhance IDIP model by including two further steps (e.g., traceback and dynamite). EMCI model involves thirteen steps (e.g., awareness, authorization, planning, notification, identify evidence, collection of evidence, transport of evidence, storage of evidence, examination of evidence, hypothesis, presentation of hypothesis, proof of hypothesis, and archive storage). DFMDFI is based on a four-tier iterative approach. The first tier deals with the preparation, identification, authorization, and communication; whereas, the second layer deals with the rules associated with collection, preservation, and documentation. However, the third tier deals with the rules related to examination, exploratory testing and analysis, and the fourth tier is responsible for providing results, reviews, and reports. SDFIM manages the digital forensic investigation process into eleven phases. ESDFIM model handles the investigation process in six phases (e.g., preparation phase, acquisition and preservation phase, examination and analysis phase, information sharing phase, presentation phase, and review phase). Further details of the above-mentioned forensic models can be found in [69].

4.7. Forensics layers

IoT forensics is composed of three layers: device, network, and cloud-level forensics. In the device level forensics, the investigator gathers evidence data mainly from IoT devices, where data are precisely stored in local memory. Network-level forensics collects data from network devices to judge or accuse a suspect. The IoT devices are usually communicate with each other through some network, i.e., LAN, WAN, MAN, PAN, etc. The networks contain useful data which can act as the trustworthy evidences such as network log data and cache memory

information. Most IoT devices have low processing and storage capabilities. They are connected to cloud data center to store or process data. Cloud forensics deals with the forensics investigation on IoT data stored at the cloud in case of attack.

4.8. Forensics tools

The forensics investigation of IoT attacks is performed by well-trained experts who have good knowledge of IT and law enforcement. Although IoT forensics involve numerous challenges, i.e., vast amount of data collection and real-time data analysis, these challenges can be compensated with the help of the various forensics tools. Computer Aided Investigative Environment (CAINE) is an interactive and open source forensics tool that supports multiple forensics phases. EnCase is utilized to perform analysis for forensics images, data, and files. **Wireshark is mostly used for network forensics analysis. The prime limitation of the Wireshark is that it does not work well with the large network data. Bulk Extractor helps to scan and extract information, e.g., card numbers, email addresses, web addresses, and telephone numbers from the disk images and directory files [54]. NUIX is used to scan a massive amount of data and processes which leads to extract the useful information later on used for the analysis purposes. RegRipper is mainly utilized to scan the Windows registry files. IEF is used to scan the forensic images and a wide range of data extracted from the Internet history, chat history, and operating systems [54]. NetAnalysis helps to scan the forensic images and data associated with the Internet history. Pajek64 helps to analyze a large amount of network-related data.**

4.9. Forensics data processing

Forensics data processing refers to the manner in which the computation location of forensics investigation is conducted. In centralized data forensics, forensics data are stored in a high-security central server that can be accessed at different locations by authorized investigators. Centralized data processing is low cost and highly secure, and it offers great control to administrators. Distributed data processing refers to

when forensics data and computation are located in distributed server. It has low latency and low delay but low security and high bandwidth requirement.

5. Use cases on IoT forensics

This section looks at different use cases with the aim of highlighting important IoT-based environments, where forensics can play an important role. Table 1 presents the summary of the use cases.

5.1. Modern flood defence systems

The United Kingdom is using modern flood defense systems. To make the system practical, sea sensors are deployed, and satellites are used gather data. These sensors and satellites correspond with each other to offer brief, computerized early water-level warnings and responses. In case of warning system failure, forensics investigation will be required to find out what and how something went wrong. In this scenario, forensics investigator can play an important role by shedding light on a part, if not all, of that picture.

5.2. Smart transport systems

Singapore is using smart transportation systems. In this context, smart sensors and other devices are deployed to manage traffic and avoid traffic congestion problem. Precision is one of the most important parameters that must be considered in smart transportation system. Incomplete and wrong information can cause serious accidents on the roads. In the case of accident, the forensics investigator is required to know what and how something went wrong. The investigation can help mitigate accident-causing issues or other problems, such as traffic congestion.

5.3. Smart health monitoring systems

In smart health monitoring systems, different types of sensing devices are used to check the health status of the person. In the case of body area network, devices transmit information to the cloud via different

Table 1: Summary of the use cases

Possible Use Case	**Description**	**Possible Evidence**	**IoT Application**	**Country**	**Forensics Need**
Modern Flood Defence Systems	Smart sea sensors are deployed to know the water level information	Smart sea sensors	Smart Sea Monitoring	United Kingdom	Yes
Smart Transportation Systems	To manage the routes in an efficient way	Smart vehicles	Smart Transport	Singapore	Yes
Smart Health Monitoring Systems	To check the health status by using the smart wearable devices	Smart wearable devices	Smart Healthcare	Global	Yes
Advanced Malware Detection in Smart Traffic Environment	To detect the malware in a smart traffic environment	Traffic lighting system	Smart Traffic	Global	Yes
Forensics Edge Management System In Smart Home	To measure the security at the edge level	Smart home appliances	Smart Home	Global	Yes

wireless technologies. A doctor uses such data to see a patient's health status through visualization approaches. An attacker may hijack the smart health monitoring system and temper the device, which can misguide the doctor while examining. Erroneous examination can cause serious health issues. The forensics investigator can play an important role in such a type of scenario.

5.4. Advanced malware detection in smart traffic environment[3]

Vulnerabilities and attack surface increase when systems become connected and integrated with other devices and various evidence types involving device-level forensics. ThreatBLADES developed a system on top of security analytics platform by Blue Coast. This device mainly aims to detect and extract files from smart traffic. ThreatBLADES is based on major protocol, which sends alerts when malware is detected and sends unknown files to a "sandbox" for dynamic malware analysis. Moreover, it offers a real-time threat intelligence service to various IoTs, which helps in increasing the efficiency of the forensic investigations. For example, HTTP, SMTP, POP3, and FTP are optimized by

[3] Accessed on: 16 April 2018 https://www.bluecoat.com/documents/download/e286d7a8-8aa1-4451-be14-d265b7ccee52/f84fbc68-1180-40a9-9d38-fe78670cd63f

each threat to detect and extract objects, such as files, URL, and IP address. ThreatBLADES also inspects categories of IoT objects.

5.5. Forensics edge management system in smart home

FEMS autonomously provides security and forensic services within the smart home. FEMS encompasses many services to provide forensics and security services within the IoT home. These services include timeline creation, compression, data parsing and differentiation, network monitoring, data mining alerting (incident escalation), result presentation, and human-understandable format reporting. Such a system is operated on the basis of IoT digital forensics framework and incorporates well-known, standardized security and forensics techniques to deliver the aforementioned services [42].

6. Requirements

This section outlines and discusses the key requirements for enabling IoT forensics successfully.

6.1. Managing IoT data volume

The volume of IoT data captured by sensors and smart devices from networks and the cloud complicate the identification of relevant data. Hence, they require proper management so they can be used as evidence for an investigation [13]. These IoT data are spread across various locations beyond the control of the investigator. In particular, capturing network traffic and managing logging performance are the important aspects in IoT forensics. The log information about the network identifies the location of evidence. Moreover, the collection and management of the IoT data may involve various locations in different countries, and information can be mixed with other users' information. The authors in [70] introduced a framework for the data storage to improve and integrate structured and unstructured IoT data efficiently. The proposed framework can store and manage diverse types of data collected by sensors and RFID readers. It can also

integrate and extend the vast number of databases, such as Hadoop distributed file system storage.

6.2. Mitigation of privacy risks

With regard to privacy, users should be aware that their data are being used for investigation. To an extent, this awareness allows users to monitor and control how and who accessed and used their data for investigation. Moreover, the investigators who are permitted to access users' data should protect the data from unauthorized access, loss, and manipulation. Leaving data unprotected can cause the investigators to be responsible for any leak and harm [13]. Mitigation of security and privacy in the context of IoT were discussed in [71]. The study highlighted several important aspects of privacy enhancement technologies to increase the security in IoT and RFID-based systems.

6.3. Integration of the IoT Data

Data integration includes all processes involved in collecting data from different sources, as well as in storing and providing data with a unified view. For each moment, different forms of data are continuously generated by social media, IoT, and other communication and telecommunication approaches [72]. Moreover, the existing tools and technologies in digital forensics domain are unable to fit with the heterogeneous infrastructure of the IoT environment. The enormous volume of promising proofs generated by a huge amount of IoT devices will subsequently require new integration guideline in terms of integrating the evidence from distributed IoT infrastructures. In [73], the authors discussed the integration of Cloud and IoT (CloudIoT). The detailed analysis of the study can help identify the complementary aspects of Cloud and IoT, which can lead to an efficient investigation during the forensics phase.

6.4. Guidelines for the IoT deployment approaches

Modern IoT smart technologies are continuously targeted by cyber attackers. User-managed smart home forensics system designed and deployed in IoT-based homes must be implemented. This system can be installed by regular network monitoring and enabling basic forensic personnel on behalf of homeowners [74]. IoT is a set of objects and sensors embedded within the networks to provide an interaction between external and internal environment via proper communications and sensing. The deployment of such technologies demands management and forensics guidelines for the application software and hardware. The researchers in [75] discussed numerous challenges related to the development of IoT business models, such as the unstructured nature of IoT systems, objects, and general immaturity.

6.5. Dealing with system identification and human behaviors

In IoT forensic, modeling of human behaviors and the extension of the system identification require new approaches and state-of-the-art predictive model to deal with shreds of evidence. Such predictive is important in generating accurate results through system identification because human behaviors evolve over time [76]. For example, identifying human faces from photos, cameras, videos are common today. Moreover, the popularity of wire, wireless and Internet communication create opportunities for identification of devices through fingerprinting [77].

7. Open Research Challenges

This section presents the challenges remaining to be addressed. It aims to provide guidelines to new researchers on IoT forensics.

7.1. Multiple locations and networks

In an IoT-based environment, user data is stored in different locations that may have multiple jurisdictions. This storage setup can raise serious complications for forensics investigators. As a consequence of different laws implementation on different locations, forensics investigators may face several problems in deciding under which rule to prosecute the cases when devices have been used in different cities or networks [78]. In a scenario where user is changing his position dynamically and using the different networks for the connectivity, investigating problems becomes challenging. In the future, standard techniques will be required to examine and analyze multiple location and network problems.

7.2. Management and automation

The use of automation in IoT forensic investigations has brought social implications and technological challenges. Such challenges come from tracking various objects and devices located at different locations, and the higher-level processes involved when a crucial piece of evidence needs to be collected from the IoT devices, such as data analysis. Moreover, to gain real-time insights into forensics investigation, automated IoT is required to improve the process time. The researchers in [42] introduced a new dimension to the forensics process, in which an automated system performs forensics investigations with end-users receiving reports as deemed necessary by the system. However, the heterogeneous nature of the IoT environment is exacting to automate due to the diversity of network devices and data being generated by IoT.

7.3. Shutting the devices down

In IoT scenario, if any device is identified as a source of generating malicious packets, stopping that device from working sometimes becomes taxing because of multiple reasons, such as the owner's individual rationality. In the case of a smart home—where a fridge is identified as a source of generating the malicious packets—the food could be spoiled if the machine is turned off. Hence, the homeowner may not allow the

investigators to turn off the fridge. This is just one of the many scenarios, e.g., transportation systems, where devices cannot be stopped from working even if something is identified as fishy for some reasons. Identifying how to handle these situations is one of the difficult tasks caused by individual rationality problem. In the future, substantial attention must be paid on designing such type of forensics mechanisms to allow forensics investigator to resolve the matter without turning off the devices.

7.4. Big IoT data analysis

The ability to analyze huge amount of IoT data assists investigators to deal with plenty of information that could have an impact on the investigation, and thus, reduce the crime rate within the city [79]. In IoT, the data are gathered from various objects, obtaining an insight into the data and making required decisions [80]. However, the higher complexity which involves in processing big IoT data hinders to perform the smooth analysis of the data available for the investigation. In addition, scalability of the analytics algorithms might have a great impact on the investigation [81]. As such, on-the-fly processing of data becomes all the more important. Traditional store-then-process approaches in which data are retrieved and stored for future access may no longer be appropriate.

7.5. Survival period and visibility of the evidences

The limitations of storage in IoT devices hinder a long-term survival of the evidence as the data can easily be overwritten, resulting in the possibility of missing evidence [14]. This challenge can be compensated by transferring data to local storage devices or on the cloud. However, it brings several new challenges, such as the difficulty to maintain a secure chain of the evidence and to prove that the evidence has not been modified. Given the deployment of thousands of sensors at the IoT crime scene, the visibility of evidence has become another crucial challenge. The possibility of implanting malicious sensors in the IoT devices can hinder the forensics investigator to identify witness devices at the crime scene. The

forensic investigator can analyze logs from the IoT devices, which can help to provide the additional information. However, such logs will not be a sufficient evidence in all cases.

7.6. Individual privacy throughout digital investigations

Despite the fact that IoT devices are facilitating humans in almost every aspect of the daily lives. However, it has been witnessed that the privacy-aware forensics solutions are lacking in the IoT paradigm. Although considerable efforts have been made towards the development of digital forensics solutions in the IoT paradigm, most of the current solutions have neglected the need for ensuring the individual privacy throughout the investigation phase [13]. For example, the forensics solutions proposed in [55, 59, 82] have some serious privacy limitations. In a highly dynamic IoT environment, the integration of privacy with the existing forensics solutions can encourage the voluntary cooperation of digital evidence which leads to understand the whole context of the situation under investigation.

7.7. Security

The pervasive nature of IoT introduces opportunities for hackers and malicious users to perform sophisticated attacks, such as sniffing, surveillance, and DoS. These attacks may be impossible to trace during the investigation. Thus, obtaining digital evidence from IoT devices for a legal purpose becomes challenging. Forensics investigations in IoT require techniques, tools, and solutions that considers IoT as a dynamic, pervasive network model composed of disparate technologies. In [83, 84], security and confidentiality were introduced. They can be used with IoT forensics based on restrictive partially blind signature scheme. This approach decreases investigators' concerns about the security implications that may affect forensic operation when IoT devices are involved.

8. Conclusion

IoT is an emerging technology that provides an unsurpassed convenience in human lives. The open interaction nature of IoT enables trillions of smart devices to share their data with one another. However, intruders can exploit such data sharing. The communication dependency of wireless technologies makes the IoT vulnerable to cyberattacks. Forensic solutions can help identify the root causes of attacks and the perpetrators. This survey aimed to explore recent studies on IoT forensics. We explained IoT's novel factors affecting traditional computer forensics. We investigated the state-of-the-art literature available on IoT forensics by analyzing their strengths and weaknesses. A taxonomy was devised by classifying the literature that can be helpful for forensic experts in selecting the most suitable choices. We discussed few indispensable use cases to show the need of forensics in different IoT applications. We also enumerated several key requirements for enabling forensics in an IoT environment. Furthermore, we discussed open research challenges related to IoT forensics as future research directions. We conclude that the current IoT systems must incorporate the forensic solutions within its architecture to ensure a safe and secure environment. Otherwise, users may undermine their trust in IoT-based systems.

9. Acknowledgment

This work was partially supported by Institute for Information communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2015-0-00557, Resilient/Fault-Tolerant Autonomic Networking Based on Physicality, Relationship and Service Semantic of IoT Devices) and the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2018-2013-1-00717) supervised by the IITP(Institute for Information communications Technology Promotion)" *Dr. CS Hong is the corresponding author.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Communications Surveys & Tutorials 17 (2015) 2347–2376.

[2] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Computer networks 54 (2010) 2787–2805.

[3] C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos, Context aware computing for the internet of things: A survey, IEEE communications surveys & tutorials 16 (2014) 414–454.

[4] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, M. Guizani, Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges, IEEE Wireless Communications 23 (2016) 10–16.

[5] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, S. Guizani, Internet-of-things-based smart cities: Recent advances and challenges, IEEE Communications Magazine 55 (2017) 16–24.

[6] T. hoon Kim, C. Ramos, S. Mohammed, Smart city and iot, Future Generation Computer Systems 76 (2017) 159 – 162.

[7] H. HaddadPajouh, A. Dehghantanha, R. Khayami, K.-K. R. Choo, A deep recurrent neural network based approach for internet of things malware threat hunting, Future Generation Computer Systems 85 (2018) 88–96.

[8] M. M. Hossain, M. Fotouhi, R. Hasan, Towards an analysis of security issues, challenges, and open problems in the internet of things, in: World Congress on Services (SERVICES), 2015, IEEE, pp. 21–28.

[9] M. A. Khan, K. Salah, Iot security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems 82 (2018) 395 – 411.

[10] F. A. Alaba, M. Othman, I. A. T. Hashem, F. Alotaibi, Internet of things security: A survey, Journal of Network and Computer Applications 88 (2017) 10–28.

[11] S. Watson, A. Dehghantanha, Digital forensics: the missing piece of the internet of things promise, Computer Fraud & Security 2016 (2016) 5–8.

[12] M. Chernyshev, S. Zeadally, Z. Baig, A. Woodward, Internet of things forensics: The need, process models, and open issues, IT Professional 20 (2018) 40–49.

[13] A. Nieto, R. Rios, J. Lopez, Iot-forensics meets privacy: towards cooperative digital investigations, Sensors 18 (2018) 492.

[14] S. Alabdulsalam, K. Schaefer, T. Kechadi, N.-A. Le-Khac, Internet of things forensics: Challenges and case study, arXiv preprint arXiv:1801.10391 (2018).

[15] R. Hegarty, D. Lamb, A. Attwood, Digital evidence challenges in the internet of things, in: Proceedings of the Tenth International Network Conference (INC 2014), Lulu. com, p. 163.

[16] Z. A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, et al., Future challenges for smart cities: Cybersecurity and digital forensics, Digital Investigation 22 (2017) 3–13.

[17] A. MacDermott, T. Baker, Q. Shi, Iot forensics: Challenges for the ioa era, in: 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018, IEEE, pp. 1–5.

[18] C. Shin, P. Chandok, R. Liu, S. J. Nielson, T. R. Leschke, Potential forensic analysis of iot data: An overview of the state-of-the-art and future possibilities, in: IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, IEEE, pp. 705–710.

[19] J. Yoon, D. Jeong, C.-h. Kang, S. Lee, Forensic investigation framework for the document store nosql dbms: Mongodb as a case study, Digital Investigation 17 (2016) 53–65.

[20] K. Barmpatsalou, T. Cruz, E. Monteiro, P. Simoes, Current and future trends in mobile device forensics: A survey, ACM Computing Surveys (CSUR) 51 (2018) 46.

[21] S. Khan, A. Gani, A. W. A. Wahab, M. A. Bagiwa, M. Shiraz, S. U. Khan, R. Buyya, A. Y. Zomaya, Cloud log forensics: Foundations, state of the art, and future directions, ACM Computing Surveys (CSUR) 49 (2016) 7.

[22] S. Khan, A. Gani, A. W. A. Wahab, M. Shiraz, I. Ahmad, Network forensics: Review, taxonomy, and open challenges, Journal of Network and Computer Applications 66 (2016) 214–235.

[23] S. Khan, M. Shiraz, A. W. Abdul Wahab, A. Gani, Q. Han, Z. Bin Abdul Rahman, A comprehensive review on adaptability of network forensics frameworks for mobile cloud computing, The Scientific World Journal 2014 (2014).

[24] M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of things security and forensics: Challenges and opportunities, Future Generation Computer Systems 78 (2018) 544 – 546.

[25] S. Khan, A. Gani, A. W. A. Wahab, A. Abdelaziz, K. Ko, M. K. Khan, M. Guizani, Software-defined network forensics: Motivation, potential locations, requirements, and challenges, IEEE Network 30 (2016) 6–13.

[26] C. Esposito, A. Castiglione, F. Pop, K.-K. R. Choo, Challenges of connecting edge and cloud computing: A security and forensic perspective, IEEE Cloud Computing 4 (2017) 13–17.

[27] N.-A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens, K.-K. R. Choo, Smart vehicle forensics: Challenges and case study, Future Generation Computer Systems (2018).

[28] E. Ahmed, I. Yaqoob, I. A. T. Hashem, I. Khan, A. I. A. Ahmed, M. Imran, A. V. Vasilakos, The role of big data analytics in internet of things, Computer Networks 129 (2017) 459–471.

[29] E. Ahmed, A. Ahmed, I. Yaqoob, J. Shuja, A. Gani, M. Imran, M. Shoaib, Bringing computation closer toward the user network: Is edge computing the solution?, IEEE Communications Magazine 55 (2017) 138–144.

[30] A. Ahmed, E. Ahmed, A survey on mobile edge computing, in: 2016 10th International Conference on Intelligent Systems and Control (ISCO), pp. 1–8.

[31] M. Tao, J. Zuo, Z. Liu, A. Castiglione, F. Palmieri, Multi-layer cloud architectural model and ontology-based security service framework for iot-based smart homes, Future Generation Computer Systems 78 (2018) 1040–1051.

[32] K. Sha, W. Wei, T. A. Yang, Z. Wang, W. Shi, On security challenges and open issues in internet of things, Future Generation Computer Systems 83 (2018) 326–337.

[33] C.-T. Kuo, P.-W. Chi, V. Chang, C.-L. Lei, Sfaas: Keeping an eye on iot fusion environment with security fusion as a service, Future Generation Computer Systems (2018).

[34] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, Z. Y. Dong, Cyber security framework for internet of things-based energy internet, Future Generation Computer Systems (2018).

[35] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, X. Yi, Privacy preserving internet of things: From privacy techniques to a blueprint architecture and efficient implementation, Future Generation Computer Systems 76 (2017) 540–549.

[36] I. Yaqoob, E. Ahmed, M. H. ur Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, M. Guizani, The rise of ransomware and emerging security challenges in the internet of things, Computer Networks 129 (2017) 444–458.

[37] Y. Lu, S. Wu, Z. Fang, N. Xiong, S. Yoon, D. S. Park, Exploring finger vein based personal authentication for secure iot, Future Generation Computer Systems 77 (2017) 149–160.

[38] M. Ammar, G. Russello, B. Crispo, Internet of things: A survey on the security of iot frameworks, Journal of Information Security and Applications 38 (2018) 8–27.

[39] X. Tang, P. Ren, Z. Han, Jamming mitigation via hierarchical security game for iot communications, IEEE Access 6 (2018) 5766–5779.

[40] B. Schneier, Iot security: What's plan b?, IEEE SECURITY AND PRIVACY MAGAZINE 15 (2017) 96–96.

[41] Q. Do, B. Martini, K.-K. R. Choo, Cyber-physical systems information gathering: A smart home case study, Computer Networks 138 (2018) 1–12.

[42] E. Oriwoh, P. Sant, The forensics edge management system: A concept and design, in: 10th International Conference on Autonomic and Trusted Computing (UIC/ATC) Ubiquitous Intelligence and Computing, 2013, IEEE, pp. 544–550.

[43] E. Oriwoh, G. Williams, Internet of things: The argument for smart forensics, Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance (2014) 407.

[44] A. Goudbeek, K. R. Choo, N. Le-Khac, A forensic investigation framework for smart home environment, in: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 1446–1451.

[45] M. Hossain, R. Hasan, S. Zawoad, Trust-iov: A trustworthy forensic investigation framework for the internet of vehicles (iov), in: 2017 IEEE International Congress on Internet of Things (ICIOT), pp. 25–32.

[46] X. Feng, E. S. Dawam, S. Amin, A new digital forensics model of smart city automated vehicles, in: International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, IEEE, pp. 274–279.

[47] M. Faheem, N.-A. Le-Khac, T. Kechadi, Smartphone forensic analysis: A case study for obtaining root access of an android samsung s3 device and analyse the image without an expensive commercial tool (2014).

[48] T. Heckmann, K. Markantonakis, D. Naccache, T. Souvignet, Forensic smartphone analysis using adhesives: Transplantation of package on package components, Digital Investigation (2018).

[49] D. R. Clark, C. Meffert, I. Baggili, F. Breitinger, Drop (drone open source parser) your drone: Forensic analysis of the dji phantom iii, Digital Investigation 22 (2017) S3–S14.

[50] Y.-Y. Teing, A. Dehghantanha, K.-K. R. Choo, L. T. Yang, Forensic investigation of p2p cloud storage services and backbone for iot networks: Bittorrent sync as a case study, Computers & Electrical Engineering 58 (2017) 350–363.

[51] N. Akatyev, J. I. James, Evidence identification in iot networks based on threat assessment, Future Generation Computer Systems (2017).

[52] J. Boucher, N.-A. Le-Khac, Forensic framework to identify local vs synced artefacts, Digital Investigation 24 (2018) S68–S75.

[53] A. Case, G. G. Richard III, Memory forensics: The path forward, Digital Investigation 20 (2017) 23–33.

[54] D. Quick, K. R. Choo, Iot device forensics and data reduction, IEEE Access (2018) 1–1.

[55] A. Nieto, R. Roman, J. Lopez, Digital witness: Safeguarding digital evidence by using secure architectures in personal devices, IEEE Network 30 (2016) 34–41.

[56] H. Chung, J. Park, S. Lee, Digital forensic approaches for amazon alexa ecosystem, Digital Investigation 22 (2017) S15–S25.

[57] M. M. Hossain, R. Hasan, S. Zawoad, Probe-iot: A public digital ledger based forensic investigation framework for iot., in: INFOCOM Workshops, pp. 1–2.

[58] V. Kumar, G. Oikonomou, T. Tryfonas, Traffic forensics for ipv6-based wireless sensor networks and the internet of things, in: Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on, IEEE, pp. 633–638.

[59] A. Nieto, R. Rios, J. Lopez, A methodology for privacy-aware iot-forensics, in: 2017 IEEE Trustcom/BigDataSE/ICESS, pp. 626–633.

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

[61] L. Perlepes, G. Stamoulis, P. Kikiras, An end–to–end framework for securing the internet of things (2011) 356–364.

[62] S. Perumal, N. M. Norwawi, V. Raman, Internet of things (iot) digital forensic investigation model: Top-down forensic approach methodology, in: 2015 Fifth International Conference on, Digital Information Processing and Communications (ICDIPC), IEEE, pp. 19–23.

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

[64] D. Lillis, B. Becker, T. O'Sullivan, M. Scanlon, Current challenges and future research areas for digital forensic investigation, arXiv preprint arXiv:1604.03850 (2016).

[65] A. Bijalwan, M. Wazid, E. S. Pilli, R. Joshi, Forensics of random-udp flooding attacks, Journal of Networks 10 (2015) 287–293.

[66] A. Sengupta, D. Kachave, Forensic engineering for resolving ownership problem of reusable ip core generated during high level synthesis, Future Generation Computer Systems 80 (2018) 29–46.

[67] J. Slay, Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques, in: Mobile Networks and Management: 9th International Conference, MONAMI 2017, Melbourne, Australia, December 13-15, 2017, Proceedings, volume 235, Springer, p. 30.

[68] M. Harbawi, A. Varol, An improved digital evidence acquisition model for the internet of things forensic: A theoretical framework, in: Digital Forensic and Security (ISDFS), 2017 5th International Symposium on, IEEE, pp. 1–6.

[69] K. Kyei, P. Zavarsky, D. Lindskog, R. Ruhl, A review and comparative study of digital forensic investigation models, in: International Conference on Digital Forensics and Cyber Crime, Springer, pp. 314–327.

[70] L. Jiang, L. Da Xu, H. Cai, Z. Jiang, F. Bu, B. Xu, An iot-oriented data storage framework in cloud computing platform, IEEE Transactions on Industrial Informatics 10 (2014) 1443–1451.

[71] R. H. Weber, Internet of things–new security and privacy challenges, Computer law & security review 26 (2010) 23–30.

[72] M. Marjani, F. Nasaruddin, A. Gani, A. Karim, I. A. T. Hashem, A. Siddiqa, I. Yaqoob, Big iot data analytics: architecture, opportunities, and open research challenges, IEEE Access 5 (2017) 5247–5261.

[73] A. Botta, W. De Donato, V. Persico, A. Pescapé, Integration of cloud computing and internet of things: a survey, Future Generation Computer Systems 56 (2016) 684–700.

[74] E. Oriwoh, P. Sant, G. Epiphaniou, Guidelines for internet of things deployment approaches–the thing commandments, Procedia Computer Science 21 (2013) 122–131.

[75] M. Westerlund, S. Leminen, M. Rajahonka, et al., Designing business models for the internet of things (2014).

[76] J. A. Stankovic, Research directions for the internet of things, IEEE Internet of Things Journal 1 (2014) 3–9.

[77] J. H. Ziegeldorf, O. G. Morchon, K. Wehrle, Privacy in the internet of things: threats and challenges, Security and Communication Networks 7 (2014) 2728–2742.

[78] J. Gill, I. Okere, H. HaddadPajouh, A. Dehghantanha, Mobile forensics: A bibliometric analysis, Cyber Threat Intelligence (2018) 297–310.

[79] Y.-Y. Teing, A. Dehghantanha, K.-K. R. Choo, Cloudme forensics: a case of big data forensic investigation, Concurrency and Computation: Practice and Experience 30 (2018) e4277.

[80] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, M. Guizani, Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges, IEEE wireless communications 24 (2017) 10–16.

[81] D. Quick, K.-K. R. Choo, Quick analysis of digital forensic data, in: Big Digital Forensic Data, Springer, 2018, pp. 5–28.

[82] A. Nieto, R. Rios, J. Lopez, Digital witness and privacy in iot: Anonymous witnessing approach, in: Proceedings of the 2017 IEEE Conference on Trustcom/BigDataSE/ICESS, Sydney, NSW, Australia, pp. 1–4.

[83] W. Zhou, Y. Jia, A. Peng, Y. Zhang, P. Liu, The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved, IEEE Internet of Things Journal (2018) 1–1.

[84] A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for iot security and privacy: The case study of a smart home, in: IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, IEEE, pp. 618–623.

Highlights

- We explore IoT's novel factors affecting traditional computer forensics.
- We investigate the state-of-the-art research on IoT forensics.
- We categorize and classify the literature by devising a taxonomy.
- We enumerate a few notable use cases related to IoT forensics.
- We outline and highlight the key requirements for enabling IoT forensics.
- We identify and discuss several indispensable open research challenges.

Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges

Ibrar Yaqoob[a], Ibrahim Abaker Targio Hashem[b], Arif Ahmed[c], S. M. Ahsan Kazmi[a], Choong Seon Hong[1a]

[a]*Department of Computer Science and Engineering, Kyung Hee University, Yongin 446-701, Korea.*
[b]*School of Computing and IT, Taylor's University, Subang Jaya, Malaysia.*
[c]*Department of Computer Science Engineering, National Institute of Technology, Silchar, India.*

Abstract

The explosive growth of smart objects and their dependency on wireless technologies for communication increases the vulnerability of Internet of Things (IoT) to cyberattacks. Cyberattacks faced by IoT present daunting challenges to digital forensic experts. Researchers adopt various forensic techniques to investigate such attacks. These techniques aim to track internal and external attacks by emphasizing on communication mechanisms and IoT's architectural vulnerabilities. In this study, we explore IoT's novel factors affecting traditional computer forensics. We investigate recent studies on IoT forensics by analyzing their strengths and weaknesses. We categorize and classify the literature by devising a taxonomy based on forensics phases, enablers, networks, sources of evidence, investigation modes, forensics models, forensics layers, forensics tools, and forensics data processing. We also enumerate a few prominent use cases of IoT forensics and present the key requirements for enabling IoT forensics. Finally, we identify and discuss several indispensable open research challenges as future research directions.

Keywords: Internet of Things, Cybersecurity, Internet of Things Forensics, Security, Cybercrime, Smart City

[1]Corresponding author.

1. Introduction

The unprecedented proliferation of miniaturized Internet of Things (IoT) devices, such as smartphones, washing machines, and medical implants, has empowered people to share information with one another [1, 2]. These devices can communicate with one another directly or via Application Programming Interface (API) over the Internet, and they can be controlled by "learned" devices with high computing capabilities, such as cloud servers, that augment smartness to low-computing devices [3–5]. The smartness and communication capabilities of IoT devices offer many beneficial applications to common people, companies, industry, and governments. IoT application is also extended in the areas of transportation, healthcare, and smart cities [6]. In addition, the market trend of IoT is increasing, as indicated by CISCO's estimation of IoT revenue, which will be around $14.4 trillion between 2013 and 2022[2]. However, emerging IoT technologies face various security attacks and threats [7]. Notable threats include virus attacks, mass surveillance, and Denial of Service (DoS) attacks, and disruption of IoT networks [8–10]. To investigate these attacks, well-trained teams must conduct digital investigation, known as IoT forensics, on the crime scene [11–13]. An illustration of security concerns in IoT-based smart environments is provided in Figure 1. The sources of evidence in IoT forensics include home appliances, cars, medical implants, sensor nodes, and tag readers, among others. In traditional forensics, the sources of evidence can be computers, mobile phones, servers, or gateways [14]. Regarding types of evidence data, IoT data can be available in any vendor-specific format, unlike in traditional forensics wherein data is mostly available in an electronic document or standard file formats [14].

IoT forensics involves many challenges due to the nonsuitability of currently available digital forensics tools and standard forensics methodologies in the IoT environment [15–18]. IoT devices also generate huge amount of various data that puzzle investigators when deciding the relevant source of evidence and identifying the exact amount of data to be used for further investigation [19].

Several surveys [20–27] were conducted previously on the usage of digital forensics in multiple domains, i.e., cloud computing, edge computing, mobile cloud computing, software-defined networks, wireless networks, smart cities,

[2] Accessed on: 17th May 2018 https://www.ironpaper.com/webintel/articles/internet-of-things-market-statistics/

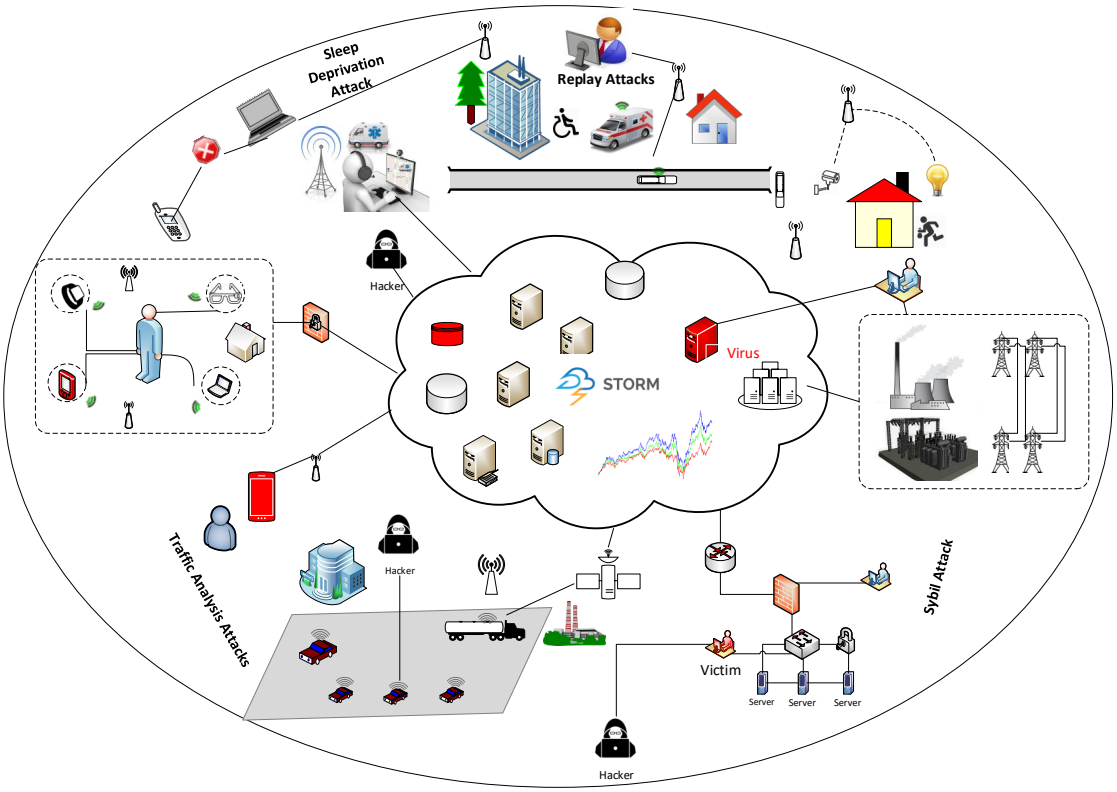

Figure 1: An illustration of security concerns in IoT-based smart environments

and smart transportation systems, among others. However, none of these surveys comprehensively focused on IoT forensics. In addition, several other important aspects of IoT forensics, which are discussed in the current study, have not been previously reported.

The contributions of this study are as follows:

- We explore IoT's novel factors affecting traditional computer forensics.
- We investigate the state-of-the-art research on IoT forensics.
- We categorize and classify the literature by devising a taxonomy.
- We enumerate a few notable use cases related to IoT forensics.

- We outline and highlight the key requirements for enabling IoT forensics.
- Finally, we identify and discuss several indispensable open research challenges.

The remainder of this paper is organized as follows. We explain IoT's novel factors affecting forensics and investigate the recent literature on IoT forensics in Sections 2–3. We discuss the devised taxonomy in Section 4, whereas we identify and present the possible use cases of IoT forensics in Section 5. Then, we outline and enumerate the key requirements for enabling IoT forensics in Section 6, followed by a discussion on several research challenges to be addressed in the IoT forensics paradigm in Section 7. Finally, we conclude the study in Section 8.

2. Novel factors of IoT affecting forensics

Numerous new factors of IoT affecting traditional computer forensics are outlined in Figure 2. A huge number of diverse and resource-constrained devices are involved in IoT-enabled environments, which generate an enormous amount of data called "Big IoT Data" [28]. A large amount of IoT data prevent the forensics investigator to collect and extract the evidence data smoothly. The main challenges posed by Big IoT Data for the forensics investigators are diverse data formats and lack of real-time log analysis solutions. Digital evidence is one of the fundamental requirements for enabling IoT forensics. Such an evidence can only be obtained by extracting firmware data or acquiring a flash-memory image. In terms of digital evidence, limited visibility and short survival period of the evidences are the new challenges posed by the IoT devices which affect the traditional computer forensic solutions to be applied in the IoT systems. In the smart environments, data are mostly stored and processed on the cloud. In most cases, acquiring access to data for investigation purposes becomes difficult for IoT forensics investigators due to service level agreement constraints. In addition, the data of IoT environment are spread across multiple platforms, e.g., on the edge devices and data centers [29, 30]. The computation is also performed mainly at the edge of users' networks,

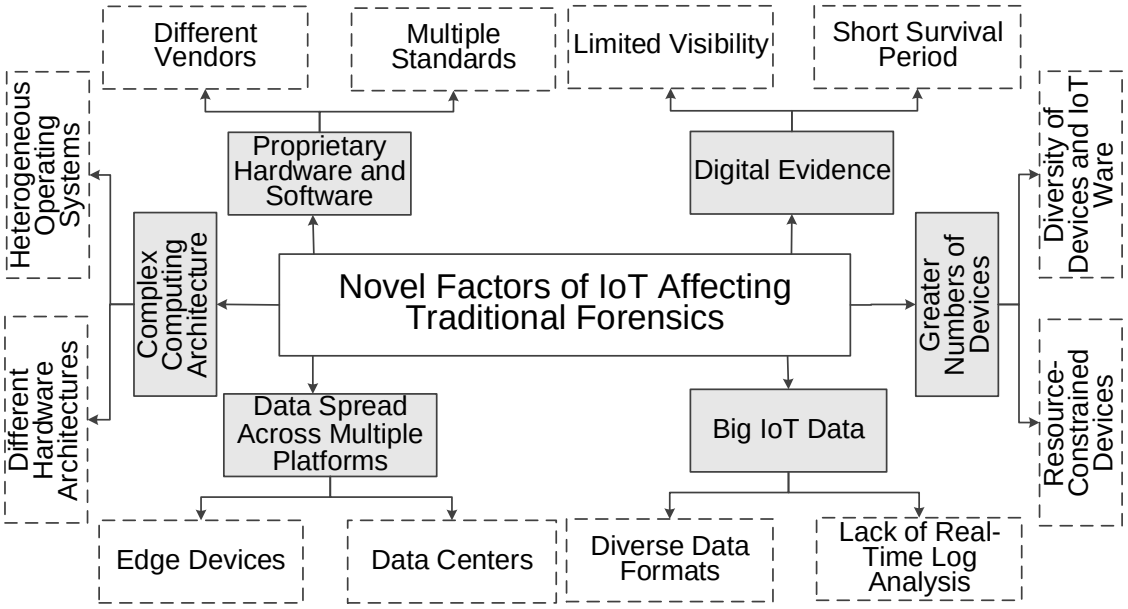

Figure 2: Novel factors of IoT affecting traditional computer forensics

and metadata are transferred to the cloud. In such a scenario, the data are stored in two hierarchies, which create difficulties for forensics investigators in terms of data collection and log data analysis. The two other IoT factors affecting forensics are complex computing architecture (i.e., different hardware architectures and heterogeneous operating systems) and proprietary hardware and software (i.e., different vendors and multiple standards).

3. Recent advances

Although many studies [31–40] are conducted on IoT security, the literature on IoT forensics is scarce. Figure 3 shows the titles of published works on IoT forensics.

3.1. Smart home forensics

Smart home devices were the focus of [41], and these devices aim to obtain compromising information. During a crime investigation, smart

Figure 3: Word frequency occurrences in most publications

home devices can play important roles through their motion detectors or microphones. These devices can help in conclusively proving a suspect's location. Three forensic adversaries were constructed, e.g., passive, active, and single-malicious active adversaries. The authors explored two smart home devices, namely, smart light and smart bulb, as case studies. The findings revealed that enormous amount of data are available to even the passive adversary, which can lead to determining the actions performed at a specific interval of time. However, this work remains in its infancy, and the solution must be automated in the future.

Forensics Edge Management System (FEMS) was designed and proposed in [42], and this system aims to provide security and forensics services for smart homes. FEMS comprises different functions, namely,

network monitoring, intrusion detection and prevention, data logging, and threshold estimation. FEMS offers numerous benefits, such as automatic detection, intelligence, and flexibility. However, its implementation involves many complexities, and its rigorous testing is taxing.

According to the authors in [43], security concerns increase as voluminous amount of devices connect to the Internet due to the vulnerabilities of smart devices. Digital forensics techniques are required to cope with such security challenges. Therefore, the authors discussed the need for digital forensics models and methodologies in the IoT paradigm (smart home). The study aimed to make arguments for the importance of smart forensics in cyber-physical environments and smart homes, as in the case of IoT. Although the authors focused mainly on the applicability of existing forensics techniques in IoT, the existing forensics techniques cannot be fully applied in IoT because of new IoT challenges, such as multiple network involvement.

In the foreseeable future, the smart home environments will become very common. In this context, a seven-phase forensic investigation framework was proposed, which can help to perform a smooth investigation in the smart home environments [44]. In the framework, phase 1 ensures that a forensics expert is available with an appropriate skills set (e.g., www.openhab.org, www.home-assistant.io). The second phase 2 ensures that all the information used in the smart home are extracted and stored safely. The next phase helps in preserving all the pieces of evidence. A global picture of the system (network topology) is created in phase 4. All the security checks are validated in phase 5. The next phase helps to locate and acquire evidential data. In the last phase, the investigator seeks to make sense of the acquired data. The applicability of the framework has been shown by presenting three case studies. The finding of the study revealed that the proposed framework can facilitate in terms of trustworthy evidence collection and preservation. However, the framework still requires to be validated using the real-world home automation systems.

3.2. Forensics analysis for smart vehicles

The Internet of Vehicles (IoV) systems enable the information sharing between the vehicles and their surrounding sensors. Although the IoV

systems have brought numerous opportunities in terms of road safety and traffic management, they brought many new challenges related to the digital forensics. To address the forensics related challenges, the study [45] has proposed a trustworthy investigation framework called Trust-IoV for the Internet of Vehicles systems. The framework helps to collect and preserve the trustworthy evidence from the highly distributed smart vehicles based environment. Furthermore, the framework helps in maintaining a secure provenance of the evidence which leads to ensuring the integrity of the stored evidence. The results of the framework suggested that the framework can operate with minimal overhead in a strong adversarial scenario. The authors in [46] investigated and analyzed the threats to smart vehicles in a smart city. A forensic model was proposed for investigating smart vehicles. Its effectiveness was affirmed by the results. However, the proposed model is in its infancy, and still requires to be validated using the data traffic generated by the smart vehicles in a real scenario.

3.3. Forensics analysis for smartphones

In the modern age of technology, people are increasingly relying on smartphones instead of desktop computers for exchanging messages, sharing videos and audios messages. A criminal can exploit the smartphone by performing a number of activities including committing a fraud over e-mail, harassment via text messages, drug trafficking, child pornography, communications related to narcotics, etc [47]. In case of exploitation, it has become very challenging to extract such information from the smartphones for the forensics purposes. To address this challenge, a study [47] is conducted which helps to perform forensic analysis for the smartphones using Universal Forensic Extraction Device (UFED) physical analyzer. The study has focused on gaining the root access and acquiring data from the Samsung Galaxy S3 phone. The purpose was to provide a vision that forensics analysis can be performed for the smartphones, however, the work was not conclusive.

Transplantation of the recent mobile phones has become a complex task involving the risk of PoP components' destruction. As such, a new solution called "PoP chip-off/TCA Technique" was proposed in [48]. The proposed technique allows the desoldering of PoP components without causing damage and ensures successful transplantation

of the latest mobile phones. A new method was also developed and successfully applied to the forensic transplantation of a cryptographic Black-Berry 9900 PGP mobile phone.

3.4. Forensics analysis for drones

A methodology that enables forensic analysis for drones was proposed in [49]. The forensic analysis was performed on DJI Phantom III drone. The study also proposed an open source tool called DRone Open Source Parser (DROP). The tool parses proprietary DAT files extracted from the drone's internal storage. These DAT files are encrypted and encoded. The work also shared preliminary findings on TXT files, which were also proprietary, encrypted, and encoded files found on the mobile device controlling the drone. The TXT files help search important information, such as GPS locations, battery, and flight time, which can be used in forensic analysis later on. Although the work helps in enabling forensic analysis in drones, it focuses only on the DJI Phantom III. Further work must be done on various types of drones, such as Phantom IV. In addition, the file structures of DAT and TXT must be demystified.

3.5. Forensics analysis for newer BitTorrent Sync peer-to-peer cloud storage

A methodology was outlined in [50], and this methodology helps in collecting and analyzing the data derived from the newer BitTorrent Sync peer-to-peer cloud storage service, which acts as a backbone for IoT networks. The experiments were performed using mobile phones, Windows-run computer systems, Mac OS, Ubuntu, iOS, and Android devices. The results revealed that artifacts relating to log-in, log-off, installation, uninstallation, and cloud synchronization metadata are recoverable. Such artifacts are considered important sources of IoT forensics. In addition, the work suggested that the memory snapshot should be obtained as quickly as possible because it increases the likelihood of preserving the artifacts. This study has many advantages, i.e., the proposed methodology can help in investigating other BitTorrent-Sync-enabled clients sharing similar datasets. However, the proposed methodology was not validated with the original equipment manufacturer.

3.6. Forensics Analysis for the General IoT Systems

A real-world investigation model for the future heterogeneous IoT systems was proposed in [51]. A threat assessment scenario was developed based on STRIDE and DREAD models. These models revealed that cyber attacks in the IoT systems can lead to serious consequences like death. Moreover, the study found that the existing solutions for the IoT systems do not include security by default, thus posing high risks. A study was conducted [52] to show the impact of the sync data on evidence. Sync data can enable impartial analysis of electronic evidence. In [53], the authors surveyed state-of-the-art in-memory forensic techniques. They explained and highlighted the important changes in designing operating systems in the future. The authors in [54] has introduced a data reduction and semi-automated investigation process, which helps in scanning the large amount of IoT data. The process helps in enabling real-time analysis of a wide range of IoT data.

The authors in [55] introduced the concept of acquiring, storing, and transmitting digital evidence reliably and securely to an authorized entity. Certain technologies that can help implement this concept in an IoT environment were discussed as well. In addition, the building blocks of the digital witness were defined. In [56], the authors proposed a new integrative approach that combines cloud-native and cloud-centric forensic for the Amazon Alexa ecosystem.

A forensic investigation framework called "Probe-IoT" was proposed in [57]. The framework helps to find criminal facts in IoT-based systems using the digital ledger, which maintains a track record of all the transactions taking place between IoT devices, users, and cloud services. The theoretical results of the framework reveal that the proposed framework ensures the integrity, confidentiality, and non-repudiation of the evidence. However, the framework has not been evaluated experimentally, and resource efficiency of the framework in terms of computation and storage cast was not analyzed. Another study[58] has proposed a traffic analysis tool, which helps to identify the attacks in IPv6 based low power wireless personal area networks. One of the prime advantages of the tool is that it presents the analysis results in a human-readable format. However, the efficiency of the tool still needs to be improved.

A new IoT forensics model called PRoFIT was proposed in [59]. This model ensures privacy (ISO/IEC 29100:2011) standard during forensic investigations. Ensuring the privacy aims to encourage IoT devices to voluntarily participate in digital forensic investigations. The proposed model was evaluated in actual malware propagation in an IoT-enabled coffee shop.

E. Oriwoh et al. [60] proposed the application of 1-2-3 zone approach to IoT-related digital forensics investigations. Persons related to the crime and possible evidence are identified in Zone 1, whereas all the devices closer to the border of the network reside in Zone 2. All devices outside the network are covered in Zone 3. In this work, the authors also introduced the next-best-thing triage model and combined it with 1-2-3 zone approach when necessary. The proposed work can provide many benefits such as effective and efficient IoT-related investigation in terms of identifying relevant evidence. However, developing and testing this work are challenging.

The researchers in [61] proposed a complete tamper-proofing framework based on three-layer architecture. The three layers are physical security mechanisms, encryption, and live forensics protection techniques. This framework provides many advantages, such as manipulation prevention, software-based protection, and infrequent verification triggering . The only disadvantage of the framework is the lack of lightweight features as most of IoT devices have limited resources in terms of battery and processing power.

The authors in [62] aimed to design the best approach in producing a novel model that enables forensics experts to conduct IoT investigations. The authors designed an integrated model based on triage and 1-2-3 zone models for volatile-based data preservation. This study was an extension of other works as it rigorously tested previous forensics investigation approaches. The proposed approach can help forensics experts conduct IoT investigations with large size-based perspective. However, the automation of this model seems rather difficult in a practical environment.

In [63], the authors introduced a new definition of IoT forensics. They also systematically analyzed IoT domain to uncover the challenges and issues in the area of digital forensics. A new approach, called Forensic-

Aware IoT (FAIoT), was proposed to support the reliability of and bring about new insights into forensic investigations in IoT environment. However, such an approach was not tested for executing digital forensics in the IoT infrastructure, which might lessen its applicability to practice.

The researchers in [64] examined the current challenges contributing to the backlog in digital forensics from a technical perspective, which can hamper the discovery of pertinent information for digital investigators. The author also highlighted a number of future research topics that could greatly contribute to a more efficient digital forensic process. As such, combined the negative effect of the challenges can be significantly amplified based on the future research works that include, information retrieval, FPGA processing, and parallelization.

A. Bijalwan et al. [65] addressed the flooding attacks against available resources in IoT environment, where the attack mode increases the difficulty of the investigation. The hackers use random-UDP flooding attacks by sending multiple UDP datagrams of different sizes at a time. This action may result in denial of services to the system and the resources. Thus, the authors proposed a new approach for the forensics investigation of random-UDP flooding attacks. This approach can identify the sources of random-UDP flooding attacks. However, this proposed solution may be unable to identify real-time attacks generated by zero-day attacks.

4. Taxonomy of IoT forensics

This section describes the taxonomy of IoT forensics illustrated in Figure 4. The attributes of this taxonomy include forensics phases, enablers, networks, sources of evidence, investigation modes, forensics models, forensics layers, forensics tools, and forensics data processing. Herein, these attributes are briefly discussed.

4.1. Forensics phases

A typical IoT forensics investigation starts with establishing context. The investigation team applies many security measurements, such software and security tools, on the vast data to be collected from different

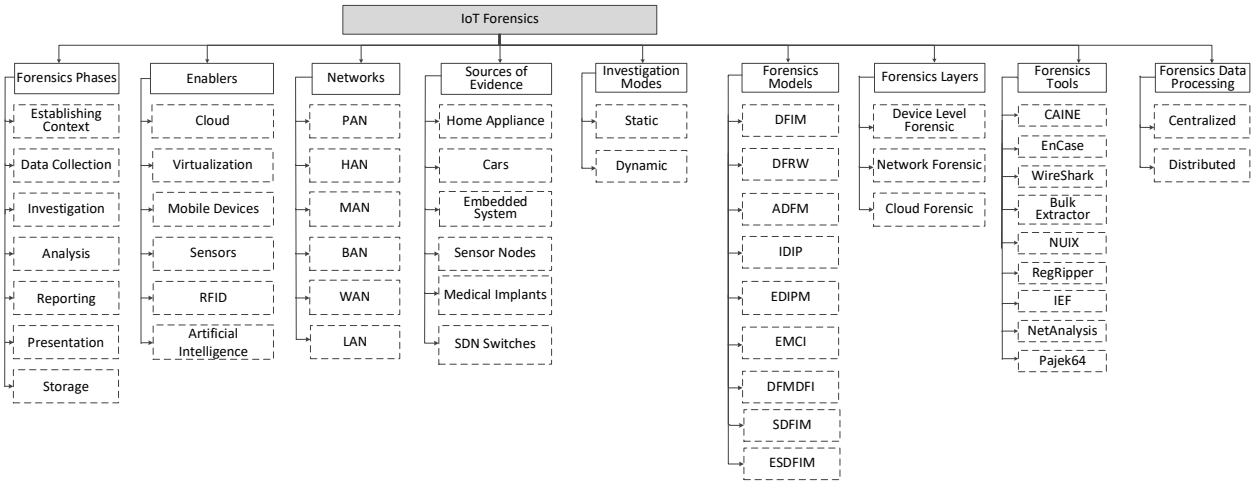

Figure 4: Taxonomy of IoT Forensics

locations [66]. The law enforcement related to the investigation, such as privacy, copyright, and information technology law, among others, are thoroughly reaffirmed and agreed by the investigator before the actual investigation. Evidence is then collected from various sources of evidence. It investigated and analyzed further in the next phase. Based on the evidence, the final conclusion is reported in the document and presented to the relevant parties. At the final phase, the collected data and the final reports are archived in a digital form for future use.

4.2. Enablers

IoT is composed of various technologies, such as sensor nodes, mobile devices, virtualization, cloud, Radio Frequency Identification (RFID), network equipment, and Artificial Intelligence (AI). These technologies play individual roles during the forensics investigation process. Core IoT devices, such as sensor nodes and mobile devices, are used to collect evidence from the crime scene after the attack. Cloud and virtualization technology provide on-demand, scalable, elastic, compute-as-a-service support during the whole forensics process. RFID is used extensively in sensor devices for object identification. Network equipment, such as routers, switches, and Software Defined Networking (SDN)

switches, enable to track packet tracing. AI techniques are used extensively in analyzing the data collected.

4.3. Networks

Network attributes refer to the type of network connected to IoT devices in the crime scene. Network type plays a great role during the investigation process, and it ensures that the area of the region is covered and law enforcement is obeyed. Local area network (LAN), Metropolitan Area Network (MAN), and Personal Area Network (PAN) are extensively used for interconnecting IoT devices within a small range. Examples of these networks are surveillance cameras installed in street and shopping malls. Home appliances, such as washing machines and refrigerators, are connected to the Home Area Network (HAN). Cloud computing plays a great role for IoT devices in terms of data storage and processing. IoT appliances are connected to the WAN network to integrate the cloud application through API.

4.4. Sources of evidence

Crime-related information in IoT can be collected from the different crime scenes focusing on the core source of evidence [67]. In IoT, the data can reside predominantly in the devices, such as home appliances, sensor nodes, medical implants, embedded systems, and cars. Although the memory spaces of IoT applications are low, valuable information is sent to the central processing computer for processing through the network. Data, such as the system log and temporary cache memory, can be used as sources of evidence. These data can be retrieved by tracing many network devices, such as routers, SDN, and switches, among others.

4.5. Investigation modes

Investigation mode categorizes the type of investigation based on the timeline of the investigation. Static mode is the traditional investigation method performed after identifying the attack in the IoT system. As a result of the attack, IoT data are already corrupted or deleted. Static mode recovers data using universal serial bus and scanning cache memory, among others. IoT forensics investigation sometimes requires

the system to be alive during the process to discover fresh data, such as open network connection, memory dumps, and running processes, for extracting important sources of evidence. This type of investigation mode is known as dynamic mode.

4.6. Forensics models

The forensics investigations for IoT applications are conducted within standard models so that the relevant evidence collected are acceptable to the court [68]. All the existing standard models follow basic phases of forensics investigation, i.e., establishing context, data collection, investigation, analysis, and reporting, among others. Digital Forensics Investigation Model (DFIM) is a four-phase model that primarily aims to uncover hidden evidence in the collected data. However, it is not concerned on actual evidence, i.e., physical evidence, which is unfavorable in IoT's case. Other existing forensic models include Digital Forensic Research Workshop (DFRW), Abstract Digital Forensic Model (ADFM), Integrated Digital Investigation Model (IDIP), Enhanced Digital Investigation Process Model (EDIPM), Extended Model of Cybercrime Investigation (EMCI), Digital Forensic Model for Digital Forensic Investigation (DFMDFI), Systematic Digital Forensic Investigation Model (SDFIM), and Enhanced Systematic Digital Forensic Investigation Model (ESDFIM) [69]. DFRW is based on seven phases (e.g., identification, preservation, collection, examination, analysis, presentation, and decision). ADFM has added three new components (e.g., preparation, approach strategy, and return of evidence), which were missing in DFRW. IDIP is a five-phase model (e.g., readiness, deployment, physical crime scene investigation, digital crime scene investigation, and review). EDIPM aims to enhance IDIP model by including two further steps (e.g., traceback and dynamite). EMCI model involves thirteen steps (e.g., awareness, authorization, planning, notification, identify evidence, collection of evidence, transport of evidence, storage of evidence, examination of evidence, hypothesis, presentation of hypothesis, proof of hypothesis, and archive storage). DFMDFI is based on four-tier iterative approach. The first tier deals with the preparation, identification, authorization, and communication; whereas, the second layer deals with the rules associated with collection, preservation, and documentation. However, the third

tier deals with the rules related to examination, exploratory testing and analysis, and the fourth tier is responsible for providing results, reviews, and reports. SDFIM manages the digital forensic investigation process into eleven phases. ESDFIM model handles the investigation process in six phases (e.g., preparation phase, acquisition and preservation phase, examination and analysis phase, information sharing phase, presentation phase, and review phase). Further details of the above-mentioned forensic models can be found in [69].

4.7. Forensics layers

IoT forensics is composed of three layers: device, network, and cloud-level forensics. In the device level forensics, the investigator gathers evidence data mainly from IoT devices, where data are precisely stored in local memory. Network-level forensics collects data from network devices to judge or accuse a suspect. The IoT devices are usually communicate with each other through some network, i.e., LAN, WAN, MAN, PAN, etc. The networks contain useful data which can act as the trustworthy evidences such as network log data and cache memory information. Most IoT devices have low processing and storage capabilities. They are connected to cloud data center to store or process data. Cloud forensics deals with the forensics investigation on IoT data stored at the cloud in case of attack.

4.8. Forensics tools

The forensics investigation of IoT attacks is performed by well-trained experts who have good knowledge of IT and law enforcement. Although IoT forensics involve numerous challenges, i.e., vast amount of data collection and real-time data analysis, these challenges can be compensated with the help of the various forensics tools. Computer Aided Investigative Environment (CAINE) is an interactive and open source forensics tool that supports multiple forensics phases. EnCase is utilized to perform analysis for forensics images, data, and files. Wireshark is mostly used for network forensics analysis. The prime limitation of the Wireshark is that it does not work well with the large network data. Bulk Extractor helps to scan and extract information, e.g., card numbers, email addresses, web addresses, and telephone numbers from the disk images and directory files [54]. NUIX is used to scan

a massive amount of data and processes which leads to extract the useful information later on used for the analysis purposes. RegRipper is mainly utilized to scan the Windows registry files. IEF is used to scan the forensic images and a wide range of data extracted from the Internet history, chat history, and operating systems [54]. NetAnalysis helps to scan the forensic images and data associated with the Internet history. Pajek64 helps to analyze a large amount of network-related data.

4.9. Forensics data processing

Forensics data processing refers to the manner in which the computation location of forensics investigation is conducted. In centralized data forensics, forensics data are stored in a high-security central server that can be accessed at different locations by authorized investigators. Centralized data processing is low cost and highly secure, and it offers great control to administrators. Distributed data processing refers to when forensics data and computation are located in distributed server. It has low latency and low delay but low security and high bandwidth requirement.

5. Use cases on IoT forensics

This section looks at different use cases with the aim of highlighting important IoT-based environments, where forensics can play an important role. Table 1 presents the summary of the use cases.

5.1. Modern flood defence systems

The United Kingdom is using modern flood defense systems. To make the system practical, sea sensors are deployed, and satellites are used gather data. These sensors and satellites correspond with each other to offer brief, computerized early water-level warnings and responses. In case of warning system failure, forensics investigation will be required to find out what and how something went wrong. In this scenario, forensics investigator can play an important role by shedding light on a part, if not all, of that picture.

Table 1: Summary of the use cases

Possible Use Case	**Description**	**Possible Evidence**	**IoT Application**	**Country**	**Forensics Need**
Modern Flood Defence Systems	Smart sea sensors are deployed to know the water level information	Smart sea sensors	Smart Sea Monitoring	United Kingdom	Yes
Smart Transportation Systems	To manage the routes in an efficient way	Smart vehicles	Smart Transport	Singapore	Yes
Smart Health Monitoring Systems	To check the health status by using the smart wearable devices	Smart wearable devices	Smart Healthcare	Global	Yes
Advanced Malware Detection in Smart Traffic Environment	To detect the malware in a smart traffic environment	Traffic lighting system	Smart Traffic	Global	Yes
Forensics Edge Management System In Smart Home	To measure the security at the edge level	Smart home appliances	Smart Home	Global	Yes

5.2. Smart transport systems

Singapore is using smart transportation systems. In this context, smart sensors and other devices are deployed to manage traffic and avoid traffic congestion problem. Precision is one of the most important parameters that must be considered in smart transportation system. Incomplete and wrong information can cause serious accidents on the roads. In the case of accident, the forensics investigator is required to know what and how something went wrong. The investigation can help mitigate accident-causing issues or other problems, such as traffic congestion.

5.3. Smart health monitoring systems

In smart health monitoring systems, different types of sensing devices are used to check the health status of the person. In the case of body area network, devices transmit information to the cloud via different wireless technologies. A doctor uses such data to see a patient's health status through visualization approaches. An attacker may hijack the smart health monitoring system and temper the device, which can misguide the doctor while examining. Erroneous examination can cause serious health issues. The forensics investigator can play an important role in such a type of scenario.

5.4. Advanced malware detection in smart traffic environment[3]

Vulnerabilities and attack surface increase when systems become connected and integrated with other devices and various evidence types involving device-level forensics. ThreatBLADES developed a system on top of security analytics platform by Blue Coast. This device mainly aims to detect and extract files from smart traffic. ThreatBLADES is based on major protocol, which sends alerts when malware is detected and sends unknown files to a "sandbox" for dynamic malware analysis. Moreover, it offers a real-time threat intelligence service to various IoTs, which helps in increasing the efficiency of the forensic investigations. For example, HTTP, SMTP, POP3, and FTP are optimized by each threat to detect and extract objects, such as files, URL, and IP address. ThreatBLADES also inspects categories of IoT objects.

5.5. Forensics edge management system in smart home

FEMS autonomously provides security and forensic services within the smart home. FEMS encompasses many services to provide forensics and security services within the IoT home. These services include timeline creation, compression, data parsing and differentiation, network monitoring, data mining alerting (incident escalation), result presentation, and human-understandable format reporting. Such a system is operated on the basis of IoT digital forensics framework and incorporates well-known, standardized security and forensics techniques to deliver the aforementioned services [42].

6. Requirements

This section outlines and discusses the key requirements for enabling IoT forensics successfully.

[3] Accessed on: 16 April 2018 https://www.bluecoat.com/documents/download/e286d7a8-8aa1-4451-be14-d265b7ccee52/f84fbc68-1180-40a9-9d38-fe78670cd63f

6.1. Managing IoT data volume

The volume of IoT data captured by sensors and smart devices from networks and the cloud complicate the identification of relevant data. Hence, they require proper management so they can be used as evidence for an investigation [13]. These IoT data are spread across various locations beyond the control of the investigator. In particular, capturing network traffic and managing logging performance are the important aspects in IoT forensics. The log information about the network identifies the location of evidence. Moreover, the collection and management of the IoT data may involve various locations in different countries, and information can be mixed with other users' information. The authors in [70] introduced a framework for the data storage to improve and integrate structured and unstructured IoT data efficiently. The proposed framework can store and manage diverse types of data collected by sensors and RFID readers. It can also integrate and extend the vast number of databases, such as Hadoop distributed file system storage.

6.2. Mitigation of privacy risks

With regard to privacy, users should be aware that their data are being used for investigation. To an extent, this awareness allows users to monitor and control how and who accessed and used their data for investigation. Moreover, the investigators who are permitted to access users' data should protect the data from unauthorized access, loss, and manipulation. Leaving data unprotected can cause the investigators to be responsible for any leak and harm [13]. Mitigation of security and privacy in the context of IoT were discussed in [71]. The study highlighted several important aspects of privacy enhancement technologies to increase the security in IoT and RFID-based systems.

6.3. Integration of the IoT Data

Data integration includes all processes involved in collecting data from different sources, as well as in storing and providing data with a unified view. For each moment, different forms of data are continuously generated by social media, IoT, and other communication and telecommunication approaches [72]. Moreover, the existing tools and technologies in

digital forensics domain are unable to fit with the heterogeneous infrastructure of the IoT environment. The enormous volume of promising proofs generated by a huge amount of IoT devices will subsequently require new integration guideline in terms of integrating the evidence from distributed IoT infrastructures. In [73], the authors discussed the integration of Cloud and IoT (CloudIoT). The detailed analysis of the study can help identify the complementary aspects of Cloud and IoT, which can lead to an efficient investigation during the forensics phase.

6.4. Guidelines for the IoT deployment approaches

Modern IoT smart technologies are continuously targeted by cyber attackers. User-managed smart home forensics system designed and deployed in IoT-based homes must be implemented. This system can be installed by regular network monitoring and enabling basic forensic personnel on behalf of homeowners [74]. IoT is a set of objects and sensors embedded within the networks to provide an interaction between external and internal environment via proper communications and sensing. The deployment of such technologies demands management and forensics guidelines for the application software and hardware. The researchers in [75] discussed numerous challenges related to the development of IoT business models, such as the unstructured nature of IoT systems, objects, and general immaturity.

6.5. Dealing with system identification and human behaviors

In IoT forensic, modeling of human behaviors and the extension of the system identification require new approaches and state-of-the-art predictive model to deal with shreds of evidence. Such predictive is important in generating accurate results through system identification because human behaviors evolve over time [76]. For example, identifying human faces from photos, cameras, videos are common today. Moreover, the popularity of wire, wireless and Internet communication create opportunities for identification of devices through fingerprinting [77].

7. Open Research Challenges

This section presents the challenges remaining to be addressed. It aims to provide guidelines to new researchers on IoT forensics.

7.1. Multiple locations and networks

In an IoT-based environment, user data is stored in different locations that may have multiple jurisdictions. This storage setup can raise serious complications for forensics investigators. As a consequence of different laws implementation on different locations, forensics investigators may face several problems in deciding under which rule to prosecute the cases when devices have been used in different cities or networks [78]. In a scenario where user is changing his position dynamically and using the different networks for the connectivity, investigating problems becomes challenging. In the future, standard techniques will be required to examine and analyze multiple location and network problems.

7.2. Management and automation

The use of automation in IoT forensic investigations has brought social implications and technological challenges. Such challenges come from tracking various objects and devices located at different locations, and the higher-level processes involved when a crucial piece of evidence needs to be collected from the IoT devices, such as data analysis. Moreover, to gain real-time insights into forensics investigation, automated IoT is required to improve the process time. The researchers in [42] introduced a new dimension to the forensics process, in which an automated system performs forensics investigations with end-users receiving reports as deemed necessary by the system. However, the heterogeneous nature of the IoT environment is exacting to automate due to the diversity of network devices and data being generated by IoT.

7.3. Shutting the devices down

In IoT scenario, if any device is identified as a source of generating malicious packets, stopping that device from working sometimes becomes

taxing because of multiple reasons, such as the owner's individual rationality. In the case of a smart home—where a fridge is identified as a source of generating the malicious packets—the food could be spoiled if the machine is turned off. Hence, the homeowner may not allow the investigators to turn off the fridge. This is just one of the many scenarios, e.g., transportation systems, where devices cannot be stopped from working even if something is identified as fishy for some reasons. Identifying how to handle these situations is one of the difficult tasks caused by individual rationality problem. In the future, substantial attention must be paid on designing such type of forensics mechanisms to allow forensics investigator to resolve the matter without turning off the devices.

7.4. Big IoT data analysis

The ability to analyze huge amount of IoT data assists investigators to deal with plenty of information that could have an impact on the investigation, and thus, reduce the crime rate within the city [79]. In IoT, the data are gathered from various objects, obtaining an insight into the data and making required decisions [80]. However, the higher complexity which involves in processing big IoT data hinders to perform the smooth analysis of the data available for the investigation. In addition, scalability of the analytics algorithms might have a great impact on the investigation [81]. As such, on-the-fly processing of data becomes all the more important. Traditional store-then-process approaches in which data are retrieved and stored for future access may no longer be appropriate.

7.5. Survival period and visibility of the evidences

The limitations of storage in IoT devices hinder a long-term survival of the evidence as the data can easily be overwritten, resulting in the possibility of missing evidence [14]. This challenge can be compensated by transferring data to local storage devices or on the cloud. However, it brings several new challenges, such as the difficulty to maintain a secure chain of the evidence and to prove that the evidence has not been modified. Given the deployment of thousands of sensors at the IoT crime scene, the visibility of evidence has become another crucial

challenge. The possibility of implanting malicious sensors in the IoT devices can hinder the forensics investigator to identify witness devices at the crime scene. The forensic investigator can analyze logs from the IoT devices, which can help to provide the additional information. However, such logs will not be a sufficient evidence in all cases.

7.6. Individual privacy throughout digital investigations

Despite the fact that IoT devices are facilitating humans in almost every aspect of the daily lives. However, it has been witnessed that the privacy-aware forensics solutions are lacking in the IoT paradigm. Although considerable efforts have been made towards the development of digital forensics solutions in the IoT paradigm, most of the current solutions have neglected the need for ensuring the individual privacy throughout the investigation phase [13]. For example, the forensics solutions proposed in [55, 59, 82] have some serious privacy limitations. In a highly dynamic IoT environment, the integration of privacy with the existing forensics solutions can encourage the voluntary cooperation of digital evidence which leads to understand the whole context of the situation under investigation.

7.7. Security

The pervasive nature of IoT introduces opportunities for hackers and malicious users to perform sophisticated attacks, such as sniffing, surveillance, and DoS. These attacks may be impossible to trace during the investigation. Thus, obtaining digital evidence from IoT devices for a legal purpose becomes challenging. Forensics investigations in IoT require techniques, tools, and solutions that considers IoT as a dynamic, pervasive network model composed of disparate technologies. In [83, 84], security and confidentiality were introduced. They can be used with IoT forensics based on restrictive partially blind signature scheme. This approach decreases investigators' concerns about the security implications that may affect forensic operation when IoT devices are involved.

8. Conclusion

IoT is an emerging technology that provides an unsurpassed convenience in human lives. The open interaction nature of IoT enables trillions of smart devices to share their data with one another. However, intruders can exploit such data sharing. The communication dependency of wireless technologies makes the IoT vulnerable to cyberattacks. Forensic solutions can help identify the root causes of attacks and the perpetrators. This survey aimed to explore recent studies on IoT forensics. We explained IoT's novel factors affecting traditional computer forensics. We investigated the state-of-the-art literature available on IoT forensics by analyzing their strengths and weaknesses. A taxonomy was devised by classifying the literature that can be helpful for forensic experts in selecting the most suitable choices. We discussed few indispensable use cases to show the need of forensics in different IoT applications. We also enumerated several key requirements for enabling forensics in an IoT environment. Furthermore, we discussed open research challenges related to IoT forensics as future research directions. We conclude that the current IoT systems must incorporate the forensic solutions within its architecture to ensure a safe and secure environment. Otherwise, users may undermine their trust in IoT-based systems.

9. Acknowledgment

This work was partially supported by Institute for Information communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2015-0-00557, Resilient/Fault-Tolerant Autonomic Networking Based on Physicality, Relationship and Service Semantic of IoT Devices) and the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2018-2013-1-00717) supervised by the IITP(Institute for Information communications Technology Promotion)" *Dr. CS Hong is the corresponding author.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Communications Surveys & Tutorials 17 (2015) 2347–2376.

[2] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Computer networks 54 (2010) 2787–2805.

[3] C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos, Context aware computing for the internet of things: A survey, IEEE communications surveys & tutorials 16 (2014) 414–454.

[4] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, M. Guizani, Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges, IEEE Wireless Communications 23 (2016) 10–16.

[5] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, S. Guizani, Internet-of-things-based smart cities: Recent advances and challenges, IEEE Communications Magazine 55 (2017) 16–24.

[6] T. hoon Kim, C. Ramos, S. Mohammed, Smart city and iot, Future Generation Computer Systems 76 (2017) 159 – 162.

[7] H. HaddadPajouh, A. Dehghantanha, R. Khayami, K.-K. R. Choo, A deep recurrent neural network based approach for internet of things malware threat hunting, Future Generation Computer Systems 85 (2018) 88–96.

[8] M. M. Hossain, M. Fotouhi, R. Hasan, Towards an analysis of security issues, challenges, and open problems in the internet of things, in: World Congress on Services (SERVICES), 2015, IEEE, pp. 21–28.

[9] M. A. Khan, K. Salah, Iot security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems 82 (2018) 395 – 411.

[10] F. A. Alaba, M. Othman, I. A. T. Hashem, F. Alotaibi, Internet of things security: A survey, Journal of Network and Computer Applications 88 (2017) 10–28.

[11] S. Watson, A. Dehghantanha, Digital forensics: the missing piece of the internet of things promise, Computer Fraud & Security 2016 (2016) 5–8.

[12] M. Chernyshev, S. Zeadally, Z. Baig, A. Woodward, Internet of things forensics: The need, process models, and open issues, IT Professional 20 (2018) 40–49.

[13] A. Nieto, R. Rios, J. Lopez, Iot-forensics meets privacy: towards cooperative digital investigations, Sensors 18 (2018) 492.

[14] S. Alabdulsalam, K. Schaefer, T. Kechadi, N.-A. Le-Khac, Internet of things forensics: Challenges and case study, arXiv preprint arXiv:1801.10391 (2018).

[15] R. Hegarty, D. Lamb, A. Attwood, Digital evidence challenges in the internet of things, in: Proceedings of the Tenth International Network Conference (INC 2014), Lulu. com, p. 163.

[16] Z. A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, et al., Future challenges for smart cities: Cybersecurity and digital forensics, Digital Investigation 22 (2017) 3–13.

[17] A. MacDermott, T. Baker, Q. Shi, Iot forensics: Challenges for the ioa era, in: 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018, IEEE, pp. 1–5.

[18] C. Shin, P. Chandok, R. Liu, S. J. Nielson, T. R. Leschke, Potential forensic analysis of iot data: An overview of the state-of-the-art and future possibilities, in: IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, IEEE, pp. 705–710.

[19] J. Yoon, D. Jeong, C.-h. Kang, S. Lee, Forensic investigation framework for the document store nosql dbms: Mongodb as a case study, Digital Investigation 17 (2016) 53–65.

[20] K. Barmpatsalou, T. Cruz, E. Monteiro, P. Simoes, Current and future trends in mobile device forensics: A survey, ACM Computing Surveys (CSUR) 51 (2018) 46.

[21] S. Khan, A. Gani, A. W. A. Wahab, M. A. Bagiwa, M. Shiraz, S. U. Khan, R. Buyya, A. Y. Zomaya, Cloud log forensics: Foundations, state of the art, and future directions, ACM Computing Surveys (CSUR) 49 (2016) 7.

[22] S. Khan, A. Gani, A. W. A. Wahab, M. Shiraz, I. Ahmad, Network forensics: Review, taxonomy, and open challenges, Journal of Network and Computer Applications 66 (2016) 214–235.

[23] S. Khan, M. Shiraz, A. W. Abdul Wahab, A. Gani, Q. Han, Z. Bin Abdul Rahman, A comprehensive review on adaptability of network forensics frameworks for mobile cloud computing, The Scientific World Journal 2014 (2014).

[24] M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of things security and forensics: Challenges and opportunities, Future Generation Computer Systems 78 (2018) 544 – 546.

[25] S. Khan, A. Gani, A. W. A. Wahab, A. Abdelaziz, K. Ko, M. K. Khan, M. Guizani, Software-defined network forensics: Motivation, potential locations, requirements, and challenges, IEEE Network 30 (2016) 6–13.

[26] C. Esposito, A. Castiglione, F. Pop, K.-K. R. Choo, Challenges of connecting edge and cloud computing: A security and forensic perspective, IEEE Cloud Computing 4 (2017) 13–17.

[27] N.-A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens, K.-K. R. Choo, Smart vehicle forensics: Challenges and case study, Future Generation Computer Systems (2018).

[28] E. Ahmed, I. Yaqoob, I. A. T. Hashem, I. Khan, A. I. A. Ahmed, M. Imran, A. V. Vasilakos, The role of big data analytics in internet of things, Computer Networks 129 (2017) 459–471.

[29] E. Ahmed, A. Ahmed, I. Yaqoob, J. Shuja, A. Gani, M. Imran, M. Shoaib, Bringing computation closer toward the user network: Is edge computing the solution?, IEEE Communications Magazine 55 (2017) 138–144.

[30] A. Ahmed, E. Ahmed, A survey on mobile edge computing, in: 2016 10th International Conference on Intelligent Systems and Control (ISCO), pp. 1–8.

[31] M. Tao, J. Zuo, Z. Liu, A. Castiglione, F. Palmieri, Multi-layer cloud architectural model and ontology-based security service framework for iot-based smart homes, Future Generation Computer Systems 78 (2018) 1040–1051.

[32] K. Sha, W. Wei, T. A. Yang, Z. Wang, W. Shi, On security challenges and open issues in internet of things, Future Generation Computer Systems 83 (2018) 326–337.

[33] C.-T. Kuo, P.-W. Chi, V. Chang, C.-L. Lei, Sfaas: Keeping an eye on iot fusion environment with security fusion as a service, Future Generation Computer Systems (2018).

[34] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, Z. Y. Dong, Cyber security framework for internet of things-based energy internet, Future Generation Computer Systems (2018).

[35] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, X. Yi, Privacy preserving internet of things: From privacy techniques to a blueprint architecture and efficient implementation, Future Generation Computer Systems 76 (2017) 540–549.

[36] I. Yaqoob, E. Ahmed, M. H. ur Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, M. Guizani, The rise of ransomware and emerging security challenges in the internet of things, Computer Networks 129 (2017) 444–458.

[37] Y. Lu, S. Wu, Z. Fang, N. Xiong, S. Yoon, D. S. Park, Exploring finger vein based personal authentication for secure iot, Future Generation Computer Systems 77 (2017) 149–160.

[38] M. Ammar, G. Russello, B. Crispo, Internet of things: A survey on the security of iot frameworks, Journal of Information Security and Applications 38 (2018) 8–27.

[39] X. Tang, P. Ren, Z. Han, Jamming mitigation via hierarchical security game for iot communications, IEEE Access 6 (2018) 5766–5779.

[40] B. Schneier, Iot security: What's plan b?, IEEE SECURITY AND PRIVACY MAGAZINE 15 (2017) 96–96.

[41] Q. Do, B. Martini, K.-K. R. Choo, Cyber-physical systems information gathering: A smart home case study, Computer Networks 138 (2018) 1–12.

[42] E. Oriwoh, P. Sant, The forensics edge management system: A concept and design, in: 10th International Conference on Autonomic and Trusted Computing (UIC/ATC) Ubiquitous Intelligence and Computing, 2013, IEEE, pp. 544–550.

[43] E. Oriwoh, G. Williams, Internet of things: The argument for smart forensics, Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance (2014) 407.

[44] A. Goudbeek, K. R. Choo, N. Le-Khac, A forensic investigation framework for smart home environment, in: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 1446–1451.

[45] M. Hossain, R. Hasan, S. Zawoad, Trust-iov: A trustworthy forensic investigation framework for the internet of vehicles (iov), in: 2017 IEEE International Congress on Internet of Things (ICIOT), pp. 25–32.

[46] X. Feng, E. S. Dawam, S. Amin, A new digital forensics model of smart city automated vehicles, in: International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, IEEE, pp. 274–279.

[47] M. Faheem, N.-A. Le-Khac, T. Kechadi, Smartphone forensic analysis: A case study for obtaining root access of an android samsung s3 device and analyse the image without an expensive commercial tool (2014).

[48] T. Heckmann, K. Markantonakis, D. Naccache, T. Souvignet, Forensic smartphone analysis using adhesives: Transplantation of package on package components, Digital Investigation (2018).

[49] D. R. Clark, C. Meffert, I. Baggili, F. Breitinger, Drop (drone open source parser) your drone: Forensic analysis of the dji phantom iii, Digital Investigation 22 (2017) S3–S14.

[50] Y.-Y. Teing, A. Dehghantanha, K.-K. R. Choo, L. T. Yang, Forensic investigation of p2p cloud storage services and backbone for iot networks: Bittorrent sync as a case study, Computers & Electrical Engineering 58 (2017) 350–363.

[51] N. Akatyev, J. I. James, Evidence identification in iot networks based on threat assessment, Future Generation Computer Systems (2017).

[52] J. Boucher, N.-A. Le-Khac, Forensic framework to identify local vs synced artefacts, Digital Investigation 24 (2018) S68–S75.

[53] A. Case, G. G. Richard III, Memory forensics: The path forward, Digital Investigation 20 (2017) 23–33.

[54] D. Quick, K. R. Choo, Iot device forensics and data reduction, IEEE Access (2018) 1–1.

[55] A. Nieto, R. Roman, J. Lopez, Digital witness: Safeguarding digital evidence by using secure architectures in personal devices, IEEE Network 30 (2016) 34–41.

[56] H. Chung, J. Park, S. Lee, Digital forensic approaches for amazon alexa ecosystem, Digital Investigation 22 (2017) S15–S25.

[57] M. M. Hossain, R. Hasan, S. Zawoad, Probe-iot: A public digital ledger based forensic investigation framework for iot., in: INFOCOM Workshops, pp. 1–2.

[58] V. Kumar, G. Oikonomou, T. Tryfonas, Traffic forensics for ipv6-based wireless sensor networks and the internet of things, in: Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on, IEEE, pp. 633–638.

[59] A. Nieto, R. Rios, J. Lopez, A methodology for privacy-aware iot-forensics, in: 2017 IEEE Trustcom/BigDataSE/ICESS, pp. 626–633.

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

[61] L. Perlepes, G. Stamoulis, P. Kikiras, An end–to–end framework for securing the internet of things (2011) 356–364.

[62] S. Perumal, N. M. Norwawi, V. Raman, Internet of things (iot) digital forensic investigation model: Top-down forensic approach methodology, in: 2015 Fifth International Conference on, Digital Information Processing and Communications (ICDIPC), IEEE, pp. 19–23.

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

[64] D. Lillis, B. Becker, T. O'Sullivan, M. Scanlon, Current challenges and future research areas for digital forensic investigation, arXiv preprint arXiv:1604.03850 (2016).

[65] A. Bijalwan, M. Wazid, E. S. Pilli, R. Joshi, Forensics of random-udp flooding attacks, Journal of Networks 10 (2015) 287–293.

[66] A. Sengupta, D. Kachave, Forensic engineering for resolving ownership problem of reusable ip core generated during high level synthesis, Future Generation Computer Systems 80 (2018) 29–46.

[67] J. Slay, Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques, in: Mobile Networks and Management: 9th International Conference, MONAMI 2017, Melbourne, Australia, December 13-15, 2017, Proceedings, volume 235, Springer, p. 30.

[68] M. Harbawi, A. Varol, An improved digital evidence acquisition model for the internet of things forensic: A theoretical framework, in: Digital Forensic and Security (ISDFS), 2017 5th International Symposium on, IEEE, pp. 1–6.

[69] K. Kyei, P. Zavarsky, D. Lindskog, R. Ruhl, A review and comparative study of digital forensic investigation models, in: International Conference on Digital Forensics and Cyber Crime, Springer, pp. 314–327.

[70] L. Jiang, L. Da Xu, H. Cai, Z. Jiang, F. Bu, B. Xu, An iot-oriented data storage framework in cloud computing platform, IEEE Transactions on Industrial Informatics 10 (2014) 1443–1451.

[71] R. H. Weber, Internet of things–new security and privacy challenges, Computer law & security review 26 (2010) 23–30.

[72] M. Marjani, F. Nasaruddin, A. Gani, A. Karim, I. A. T. Hashem, A. Siddiqa, I. Yaqoob, Big iot data analytics: architecture, opportunities, and open research challenges, IEEE Access 5 (2017) 5247–5261.

[73] A. Botta, W. De Donato, V. Persico, A. Pescapé, Integration of cloud computing and internet of things: a survey, Future Generation Computer Systems 56 (2016) 684–700.

[74] E. Oriwoh, P. Sant, G. Epiphaniou, Guidelines for internet of things deployment approaches–the thing commandments, Procedia Computer Science 21 (2013) 122–131.

[75] M. Westerlund, S. Leminen, M. Rajahonka, et al., Designing business models for the internet of things (2014).

[76] J. A. Stankovic, Research directions for the internet of things, IEEE Internet of Things Journal 1 (2014) 3–9.

[77] J. H. Ziegeldorf, O. G. Morchon, K. Wehrle, Privacy in the internet of things: threats and challenges, Security and Communication Networks 7 (2014) 2728–2742.

[78] J. Gill, I. Okere, H. HaddadPajouh, A. Dehghantanha, Mobile forensics: A bibliometric analysis, Cyber Threat Intelligence (2018) 297–310.

[79] Y.-Y. Teing, A. Dehghantanha, K.-K. R. Choo, Cloudme forensics: a case of big data forensic investigation, Concurrency and Computation: Practice and Experience 30 (2018) e4277.

[80] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, M. Guizani, Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges, IEEE wireless communications 24 (2017) 10–16.

[81] D. Quick, K.-K. R. Choo, Quick analysis of digital forensic data, in: Big Digital Forensic Data, Springer, 2018, pp. 5–28.

[82] A. Nieto, R. Rios, J. Lopez, Digital witness and privacy in iot: Anonymous witnessing approach, in: Proceedings of the 2017 IEEE Conference on Trustcom/BigDataSE/ICESS, Sydney, NSW, Australia, pp. 1–4.

[83] W. Zhou, Y. Jia, A. Peng, Y. Zhang, P. Liu, The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved, IEEE Internet of Things Journal (2018) 1–1.

[84] A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for iot security and privacy: The case study of a smart home, in: IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, IEEE, pp. 618–623.

IBRAR YAQOOB is currently working as a Postdoctoral researcher at Kyung Hee University, South Korea. He received his Ph.D. (Computer Sciences) from the University of Malaya, Malaysia, in 2017. Prior to that, he received his BS. IT (Hons.) degree from the University of the Punjab, Gujranwala Campus, Pakistan, in 2012. He worked as a researcher at the Centre for Mobile Cloud Computing Research (C4MCCR), University of Malaya. His numerous research articles are very famous and among the most downloaded in top journals. He is currently serving/served as a guest/associate editor in various Journals. He has been involved in a number of conferences and workshops in various capacities. His research interests include big data, edge computing, mobile cloud computing, the Internet of Things, computer networks, and software-defined networks.

IBRAHIM ABAKER TARGIO HASHEM is working as a faculty member in Taylor's University, Malaysia. He received his Ph.D. (computer science) from the University of Malaya in 2017. He received his M.S. degree in computing in 2012 and his B.E. degree in computer science in 2007. He obtained professional certificates from CISCO (CCNP, CCNA, and CCNA Security) and APMG Group (PRINCE2 Foundation, ITIL v3 Foundation, and OBASHI Foundation). His main research interests include big data, cloud computing, distributed computing, and networks.

ARIF AHMED received his M.Tech. degree in computer science and engineering from the National Institute of Technology Silchar, India, in 2014, and B.Tech. in information technology (with rank) from Assam University, Silchar, India, in 2012. He worked as a visiting scientist at the Centre for Development of Advanced Computing, Mumbai, India, from 2014 to 2015. From 2015 onward he has been working as an assistant professor at the National Institute of Technology Silchar. His research interests are in the field of mobile cloud computing, fog computing, software-defined networking, and mathematical modeling.

S. M. AHSAN KAZMI received his Master's degree in Communication System Engineering from the National University of Sciences and Technology (NUST), Pakistan, in 2012, and his Ph.D. degree in Computer Science and Engineering from Kyung Hee University, South Korea, in 2017. His research interests include applying analytical techniques of optimization and game theory to radio resource management for future cellular networks.

CHOONG SEON HONG received the B.S. and M.S. degrees in electronic engineering from Kyung Hee University, Seoul, South Korea, in 1983 and 1985, respectively, and the Ph.D. degree from Keio University, Minato, Japan, in 1997. In 1988, he joined Korea Telecom, where he worked on broadband networks as a Member of Technical Staff. In September 1993, he joined Keio University. He worked for the Telecommunications Network Laboratory, Korea Telecom, as a Senior Member of Technical Staff and the Director of the Networking Research Team until August 1999. Since September 1999, he has been a Professor with the Department of Computer Science and Engineering, Kyung Hee University. His research interests include future Internet, ad hoc networks, network management, and network security. He is a member of ACM, IEICE, IPSJ, KIISE, KICS, KIPS, and OSIA. He has served as the General Chair, a TPC Chair/Member, or an Organizing Committee Member for international conferences such as NOMS, IM, AP-NOMS, E2EMON, CCNC, ADSN, ICPP, DIM, WISA, BcN, TINA, SAINT, and ICOIN. In addition, he is currently an Associate Editor of the IEEE Transactions on Network and Service Management, International Journal of Network Management, and Journal of Communications and Networks and an Associate Technical Editor of the IEEE Communications Magazine.