The Internet of Things: Challenges and considerations for cybercrime investigations and digital forensics

Áine MacDermott[1], Thar Baker[1], Paul Buck[1], Farkhund Iqbal[2], Qi Shi[1]
[1]*Liverpool John Moores University, UK*
[2]*Zayed University, Abu Dhabi, UAE*

ABSTRACT

The Internet of Things (IoT) represents the seamless merging of the real and digital world, with new devices created that store and pass around data. Processing large quantities of IoT data will proportionately increase workloads of data centres, leaving providers facing new security, capacity and analytics challenges. Handling this data conveniently is a critical challenge, as the overall application performance is highly dependent on the properties of the data management service. This paper explores the challenges posed by cybercrime investigations and digital forensics concerning the shifting landscape of crime – the IoT and the evident investigative complexity – moving to the Internet of Anything (IoA)/Internet of Everything (IoE) era. IoT forensics requires a multi-faceted approach where evidence may be collected from a variety of sources such as sensor devices, communication devices, fridges, cars and drones, to smart swarms and intelligent buildings.

Keywords: Computer Forensics, Mobile Forensics, Internet of Things, IoT, Internet of Anything, Internet of Everything, Forensic Analysis, Cybercrime Investigations, Digital Forensics.

INTRODUCTION

Crime has always been a part of human society, but the means by which these crimes are committed are constantly developing and expanding. The evolving nature of technology supports criminals with new methods and tools to commit crimes. Previously, criminal investigations generally relied on the analysis of physical evidence, the study of the crime scene, speaking to and taking statements from witnesses, and interviews with suspects. Today, the criminal investigator must recognise that the evidence they have to analyse could be in an electronic or digital form (Macdermott, Baker, & Shi, 2018). The crime scene may comprise a computer system, smart and small-scale digital devices or network traffic/logs as opposed to the traditional 'physical' scene. The 'witnesses' in these cases may be computer-generated log files, metadata, or browsing history. You can prove with forensic science that someone was holding a certain weapon via DNA/fingerprints, but how do we prove that a particular suspect was the one at the keyboard at the time the crime was committed? Forensic linguistics is increasingly used within this domain to facilitate investigations by identifying actors within an exchange, determine motive and behaviours, and establish a timeline of events.

Technological developments and our increased interconnection to the Internet, and devices in our everyday lives, lead to the increase in cybercrimes. These developments and the anonymity that comes from the Internet serve as incentive for criminals, and thus lead to an increase in crimes involving

computers and cybernetics. Cybercrime is a broadly defined term, which means "criminal activities carried out by computers or the Internet" (McMurdie, 2016) and consists of three main components:

- The computer used as a tool for committing the crime;
- The computer is a repository for information used or generated in the commission of a crime;
- Information residing on the computer is the target of the crime, with the intention of damaging its integrity, confidentiality or availability.

The anonymity of the Internet can create a feeling of distance, so often criminals feel removed from their crimes or have a feeling of dissociative ignorance to the effects their actions have on others. There were approximately 3.6 million cases of fraud and two million computer misuse offences in 2017, according to an official survey by The Office for National Statistics (Casciani, 2017). Cybercrime is increasingly affecting a variety of domains: government systems, large organisations, small-to-medium enterprises (SMEs), ecommerce, online banking, and critical infrastructure. Motivations differ, but cybercrime for gain is significant, much more significant than the perception of non-economic attacks, but much less in terms of volume of attempts or reported cases. The key concerns include damage to reputation, monetary loss, and effects to the confidentiality, integrity and availability of data.

With this evident increase in cybercrime, a significant challenge from an investigative standpoint is the mass of devices that can be utilised for committing the crime, and the amount of "devices of interest" to be identified, collected, and analysed at a crime scene. These devices vary in technological complexity and storage capabilities, and range from smart phones to smart watches, smart toys, gaming consoles (Xbox One, Sony PlayStation - PS3 and PS4), health wearables and drones. The increasing utilisation of cloud services in their day-to-day operations by organisations, utilisation of huge storage devices (e.g., Redundant Array of Interdependent Disk (RAID)) and the heightened emergence of smart device utilisation means that digital forensic investigations involving such systems would involve more complex digital evidence acquisition and analysis (Taylor, Haggerty, Gresty, & Hegarty, 2010). While developing standards to deal with electronic or digital evidence, it is necessary that other supporting disciplines must also evolve to assist the investigator in this new realm and ensure they are knowledgeable on suitable conduct at the crime scene.

As we look ahead to a world of expanding ubiquitous computing, the interconnection of 'Things' to an 'Internet of Things', the challenge of forensic processes such as data acquisition (both logical and physical) and extraction and analysis of data grows in this space. The main purpose of this article is to explore the key contributors to this paradigm shift and illustrate how cybercrime investigations and digital forensics are adjusting to this new wave of cybercrime. Objectives for exploring this technological advancement begin by illustrating the progression of digital forensics – from the infant computer forensics, to mobile forensics, to network/Cloud forensics – and how the focus is now shifting to IoT forensics, and inevitably IoA/IoE forensics. Imperative to this is the identification of the range of devices now involved in digital forensic investigations, making forensic processes more challenging and problematic. Future directions within the field of digital forensics and considerations are presented. The rest of the paper is organised as follows: the next section provides background on digital forensics and cybercrime investigation and the IoT paradigm is adding to the complexity, followed by digital forensics methodologies and procedures for various evidences, then potential challenges and considerations with concluding remarks and future directions.

BACKGROUND

The term '*digital forensics'* was originally used as a synonym for computer forensics but has expanded to include an investigation of all devices capable of storing, processing and transmitting digital data. With

roots in the personal computing revolution of the late 1970s and early 1980s, the discipline evolved in a disorganised manner during the 1990s, and it was not until the early 21st century when its prominence was realised (Hausknecht & Gruičić, 2017). Despite the field's quick evolution, advancement in digital forensics is now more difficult to achieve. Its evolution is challenged heavily by the increasing popularity of digital devices and the heterogeneity of the hardware and software platforms used. For example, the plethora of file formats and operating systems (OSs) impede the creation of unified or standard tools, and the advent of smartphones that extensively use cryptography or embed digital rights management/trusted computing frameworks make collecting evidence a complex task (Caviglione, Wendzel, & Mazurczyk, 2017).

At a cybercrime investigation, digital forensic analysts scrutinise seized data and explain the current state of the digital artefact(s). Cybercrime investigations follow the standard digital forensic process and the investigations are performed on static data, in the form of digital images that have been taken using specialist software, such as FTK Imager or EnCase Forensic Imager. Typical forensic analysis includes a manual review of the material on the media and filtering files of suspicion. Reviewing the registry for suspicious information is an additional action, as is using keyword searches for evidence related to the offence in the hope that files of suspicion are found – which is a lengthy and time-consuming process. Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every type of crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. It has a vital role in information assurance – investigations of security breaches yield valuable information that can be used to design more secure and resilient systems (Liu, Singhal, & Wijesekera, 2017).

Network forensics techniques assist in tracking internal and external network attacks by focusing on the devices present and the communication mechanisms applied. Many network attacks are designed to block users from accessing services and providers from delivering services, i.e., Denial of Service (DoS) or Distributed Denial of Service (DDoS). Critical security issues include data integrity, user confidentiality, data and service availability, and trust among entities. Securing applications and services provided in the Cloud against cyber-attacks is hard to achieve due to the complexity, heterogeneity, and dynamic nature of such systems (Macdermott, Shi, & Kifayat, 2017). Network forensics involves identifying, capturing, discovering, and analysing network devices as well as infrastructure (Khan, Gani, Wahab, Shiraz, & Ahmad, 2016). The purpose of such an analysis is to explore digital evidence in the network traffic after the occurrence of a suspicious event. In a larger scale environment, it is the ability to sift through gigabytes of the captured network traffic and construct multiple views of that traffic benefits network security, policy enforcement, and network maintenance personnel (Corey, Peterman, Shearin, Greenberg, & Van Bokkelen, 2002). Cloud forensics is an emerging branch of network forensics, which involves post-incident analysis of systems with distributed processing, multi-tenancy, virtualisation and mobility of computations (Liu et al., 2017). In the virtual environments provided in a cloud computing system, digital forensic investigations can be troublesome due to its dynamic nature. If a software application is accessed via a cloud computing system, data is traditionally written to the OS. Evidence can be acquired in the form of registry entries or temporary Internet files, which would reside or be stored within the virtual environment and so get lost when the user exits the cloud.

Digital forensics is becoming more challenging due to the tremendous increase in computing devices and computer-enabled paradigm, providing new challenges to the distributed processing of digital data and adding to the investigative complexity. The IoT foresees the Internet as a set of intelligent, self-configuring, and interconnected objects in a dynamic and global infrastructure. These 'Things' or 'Objects' refer to uniquely addressable smart devices that are generally distributed endowed with sensing and actuation capabilities and equipped with limited computing resources such as CPU, memory, and

network capabilities. This is evidently an integration of several technologies and communication solutions such as Radio Frequency Identification (RFID) technology, sensors and actuators (Baker, Asim, Tawfik, Aldawsari, & Buyya, 2017). To effectively deal with this fundamental change in evidence, the science of digital forensics is developing. The objective is still the same as in physical crime scenes; determining the crime, identifying and analysing the evidence, and establishing the party or parties involved. While developing standards for dealing with electronic or digital evidence, it is necessary that other supporting disciplines must also evolve to assist the investigator (Rogers, 2003). As of now, there is a standardised method for retrieving evidence from traditional devices such as hard drives and mobile phones but no clear procedures for IoT-based investigations, which we believe will require a multi-faceted approach. There are no defined principles for IoT forensics as the sphere of "devices of interest/potential evidence" continues to grow, as such; investigations will significantly rely on the mechanical and physical nature of the smart device, since evidence fingerprinting is a major challenge. Evidence can be collected from fixed sensors in homes and buildings, moving sensors built into cars and wearable devices, communication devices, cloud storage and even ISP logs.

CYBERCRIME INVESTIGATIONS AND DIGITAL FORENSICS

Digital forensics has become an important tool in the fight against cybercrime via identification of computer-based and computer-assisted crime. Today's huge volumes of data, heterogeneous information and communication technologies, and borderless cyber infrastructures create new challenges for security experts and law enforcement agencies investigating cybercrimes. Pursuing cybercrime investigations can span international borders, jurisdictions, and legal systems. This issue, jointly with the huge volume and richness of information, highly heterogeneous ICT technologies, and complex modern hardware/software frameworks, raises new challenges, especially in digital forensics (Caviglione et al., 2017). Digital forensic investigations are ubiquitously utilised within law enforcement to investigate electronic media and increasingly within organisations as part of their incident response procedures (Al Fahdi, Clarke, & Furnell, 2013). Historically, the impact of e-crime or computer related crime has involved only a small proportion of victims and investigators. However, this position is changing and the impact of digital evidence within 'conventional' investigations is already widespread. Any investigation within the public or private arena is likely to involve the seizure, preservation and examination of electronic evidence, therefore digital evidence processing must form an integral part of the wider investigative process.

A 'digital forensics process model' or 'digital forensic methodology' provides a framework for procedures and processes that should be followed when engaging in a digital forensics-based investigation. An increasing number of models have been proposed, attempting to speed up the investigative process or to solve problems encountered during the forensic investigation (Du, X., Le-Khac, N. A., & Scanlon, 2017). Mocas identified the following standards for digital evidence: Duplication integrity, Authentication, Reproducibility, Non-interference, Identifiable non-interference, and Minimisation. These properties and terms establish principles for research and tools development (Mocas, 2004). For crime scene processing and evidence confiscation, the use of model or methodology is dependent upon the investigator. There are many models to choose from, each comprising the same main stages (identify, secure, analyse, present), but with differing attention focusing on different stages. For example, the "Advanced Data Acquisition Model" (ADAM) methodology (Adams, 2013) allocates considerable time for pre-planning and pre-investigative stages. The aim of the ADAM is to address the shortcomings identified in a previous review study (Adams, 2012), revealing that none of the currently available models meet the needs of practitioners and researchers.

Current models are criticised from different aspects, such as being too specific (Reith, M., Carr, C., & Gunsch, 2002), too broad (Rogers, 2006), or too complex (Selamat, S. R., Yusof, R., & Sahib, 2008). In contrast, "CFSAP" (Computer Forensics – Secure, Analyse, Present) comprises the four key elements of

computer forensics (identification, preservation, analysis, and presentation) into three steps to follow: Secure (identify sources of digital evidence, preserve digital evidence), Analyse (forensic analysis of digital evidence: extract, process, interpret), Present (Presentation of digital evidence, expert opinion and testimony) (Macdermott et al., 2018). "Framework for Reliable Experimental Design" (FRED) proposed by Horsman, focuses on the underpinning procedures involved within undertaking the reverse engineering of digital data structures and the process of extracting and interpreting digital content in a reliable way. The proposed framework is designed to be a resource for those operating within the digital forensic field, both in industry and academia, to support and develop research best practice within the discipline (Horsman, 2018). Regardless of approach, the three key stages are the collection, analysis, and presentation of evidence, but the level of emphasis and attention on other stages can differ. Depending on the scenario, there could be a need to pay more attention to other stages or to adapt the approach. There is a need for standardisation and transparency in digital forensic research methodologies to allow sufficient peer-review of practices, secondary interpretation of data and the ability to assess the reliability of findings that are offered in any contribution to knowledge (Horsman, 2018). Following a general process model is not specific enough to deal with the different types of cybercrime and the broad range of cases encountered by law enforcement.

The ACPO (Association of Chief Police Officers) guide (ACPO, 2012) underpins the current actions undertaken by investigators, regardless of forensics methodology followed within the United Kingdom. The ACPO guide details instructions for the investigator to legally obtain and analyse the evidence, but as the evidence can come in many forms and there are many scenarios, which this evidence may be involved in, there needs to be an effective framework to support this. With this reasoning, the investigator at the crime scene must follow the guidelines set by ACPO ensuring analysis of the data occurs, collecting all relevant data in an efficient and resourceful manner. The ACPO guide lists principles for computer-based electronic evidence and is listed below (ACPO, 2012):

- Principal 1: "No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court."
- Principal 2: "In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions."
- Principle 3: "An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result."
- Principle 4: "The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to."

These principles, if followed, allow the investigator to lawfully obtain and analyse the evidence, and maintain a good chain of custody. Much of the last decade's progress concerning the shifting landscape of crime is quickly becoming irrelevant according to Garfinkel (Garfinkel, 2010) presenting "Digital Forensics Research: The Next 10 Years" at the Digital Forensics Research Conference in 2010. Garfinkel argues, "*We have been in a "Golden Age of Digital Forensics," and that the Golden Age is quickly coming to an end. Increasingly organisations encounter data that cannot be analysed with today's tools because of format incompatibility, encryption, or simply a lack of training*." The main issues identified by Garfinkel are concerned with the growing size of devices of interest, the size of storage devices (meaning longer time spent creating a forensic image), and the proliferation of OSs and file formats, which is increasing the requirements and complexity of forensic analysis tools and procedures. In the infancy of computer forensics, cases were limited to the analysis of a single device; increasingly cases require the analysis of multiple devices followed by the correlation of the collected evidence. Issues identified within the study are still prominent now in 2018 (Horsman, 2018), and the rapid embrace of the IoT/IoA era enhances these concerns (Macdermott et al., 2018).

IoT-based forensic investigations need to identify, preserve, analyse, and present the digital evidence collected from the IoT components. The changing landscape requires well-defined accredited tools, adaptive frameworks, and dynamic solutions tailored to the IoT/IoA paradigm. When an IoT device is identified, there is no documented method or a reliable tool to collect residual evidences from the device in a forensically sound manner. In addition, there are very limited methods to create a forensic image of a given IoT device ignoring ethical considerations when collecting evidences from devices running in a multi-tenancy environment. There can be masses of data to analyse, as the amount of digital media, storage masses can range from individual to individual, and the analysis and scrutiny of these can be extremely time consuming, especially when there is no clear objective in the case initially. The rapid implementation of connectivity in industrial control processes in critical systems, across a wide range of industries such as energy, mining, agriculture and aviation, has created the "*Industrial Internet of Things*" – IIoT. This is simultaneously opening up the possibility of new devices and processes, which were never vulnerable to such interference in the past, being hacked and tampered with, with potentially disastrous consequences (Hammond, 2016).

Table 1. Forensic evidence per digital forensics 'category'

	Forensic evidence
Computer	The identification, preservation, collection, analysis and reporting on evidence found on computers, laptops, and removable storage media.
Mobile	The recovery of evidence from mobile phones, smartphones, SIM cards, PDAs, GPS devices, tablets, smart toys, wearables, drones and game consoles.
Network	The monitoring, capture, storing and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents. Mechanisms include traceback, logging, packet marking, reference heuristic base, packet analysis (dependent upon network monitoring setup).
Cloud	Evidence can be distributed across several machines, most of which would be outside the control of the investigator, e.g., social network logs, ISPs, data in transit, online storage media, data stored by mobile network providers. Other challenges include the dependence of forensically-valuable data on the cloud deployment model, large volumes of data, proprietary data formats, multiple isolated virtual machine instances running on a single physical machine and inadequate tools for conducting cloud forensics (Liu et al., 2017). Everything online means potential evidence too is stored in the cloud and not just locally on the device: • Usage logs from smart homes. • Connection logs from smart buildings. • GPS data from smart cars/traffic sensors/utility devices.
IoT	The recovery of evidence from devices locally (depending upon IoT device) but this could also encompass mobile/network/Cloud forensics. Examples include fixed sensors in homes and buildings, moving sensors built into cars, wearable devices, communication devices, cloud storage, ISP logs, drone data, wearable technology.

Table 1 presents forensic evidence per digital forensics 'category' – Computer-based, Mobile-based, Network-based, Cloud-based and IoT-based. Compared to traditional digital forensics, there is less certainty in where data originated from, and where it is stored, so data persistence may be a problem (Lillis, Becker, O'Sullivan, & Scanlon, 2016). Evidence extraction and analysis is also an issue with IoT devices. In IoT scenarios, persistent recording is not easily achieved due to resource constraints in embedded systems, or smart objects with limited memory and computing. IoT devices differ not only in their type but also in accessibility and interfaces, vendor-specific features, and data storage (local versus cloud-based and persistent versus volatile) (Caviglione et al., 2017). Future digital forensics tools and techniques should be engineered to support heterogeneous investigations, preserve privacy, and offer scalability. New tools are necessary to improve IoT forensics, especially because anti-forensic techniques will continue to become increasingly sophisticated (Caviglione et al., 2017). Currently digital forensic and

cyber security experts are exploring the IoT from the perspective of a digital forensic analyst concerning evidence handling, evidence extraction, and analysis of the collected data. Many questions have yet to be answered in this emerging area. Using innovative technologies, alongside the knowledge acquired from these studies as a starting point for understanding the IoT world and IoT-ware will help in answering these questions and guiding the industry with more knowledge on IoT forensics. With the new types of devices that are part of the IoT, we must determine the best approach for ensuring they are examined in the same forensically sound manner. Evidence prioritisation via advancing crime scene methodologies and process models is essential.

CASE STUDY: CRIME SCENE CONSIDERATIONS AND CHALLENGES

Digital forensics investigations undertaken by high-tech crime units or law enforcement can involve analysts with varying skillsets. While there are new and emerging technologies increasingly being used to commit crime, there could be miscommunication on the handling of these devices, which could affect ongoing cases and use of seized evidence in court. Additionally, search and seizure procedures used in the conventional computer forensic process are usually not applicable due to evidence being stored in cloud datacenters. As the digital revolution advances, consumer attitudes, beliefs and intentions have continued to evolve – more consumers are turning their homes into 'smart' homes or introducing IoT-enabled devices into their home. As such, within an IoT-based crime scene, there are a range of devices that could be located on site. Examples of potential IoT-based evidence include smart home assistants, e.g. Amazon Alexa (it could contain correspondence between smart assistants at other homes, or recent voice commands), home appliances, heating control, lighting, smart energy meters, smart plugs, doorbells, security, to name a few. Regardless of the circumstance of the investigation, there could be data residing on one or more of these devices that is vital to a case, be it, corroborating an alibi, or determining the device was used for something illegal or malicious. Additionally, compatibility and interoperability between devices is not as readily available as it seems, so many of these devices are controlled via mobile app, or through the smart home assistant. They may also be connected to different networks within the same location, or connected to another location nearby. Prior to attending a crime scene, if details are missing from the terms of the warrant, vital pieces of evidence may be missed.

The main IoT/IoA challenge from a digital forensic perspective is that of data imaging and acquisition – knowing exactly where the data is and actually acquiring the data (Macdermott et al., 2018). It is also difficult to maintain a clear chain of custody relating to the acquisition of the evidence. Essentially, IoT/IoA means that investigators are unable to conform to the ACPO guide, as it is difficult if not impossible to satisfy all ACPO principles (if the investigation is based within the UK). Almost every digital forensic investigation model should start with authorisation, planning and obtaining a warrant as this is fundamental and can be assumed as a proper standard operating procedure, leading into a strategy to navigate the digital forensic investigation further (Oriwoh, Jazani, Epiphaniou, & Sant, 2013).

Cybercrime investigators are often overwhelmed with the mass of digital evidence, so identification of items of forensic interest can be time consuming. As the digital age continues to produce an ever-increasing variety of digital evidence – from drones, USB drives, CCTV footage, Micro SD cards, Xboxes, hard drives, to the broad array of mobile phones, can cause substantial case backlogs due to the individual scrutiny of device (Dolliver, Collins, & Sams, 2017). From a police perspective, this can slow down the progression of the case to the court of law where the digital evidence may be pinnacle to the case. Data integrity checking, which is the core of digital forensic process is another challenge, which is lacking uniformity due to different data imaging and acquisition approaches employed by different stakeholders at different locations performed with heterogeneous tools. Cross integrity checking and verifiability of imaged evidence in a situation where different stakeholders such as ISP, cloud service provider, law enforcement, digital forensics company are jointly working on the same forensic case will

remain an open question for investigators. We believe blockchain technology could be an efficient and accurate way to maintain integrity of evidence and have a clear chain of command in a collaborative investigation, but the applications will be considered in future investigations.

Encryption and cloud computing both threaten forensic visibility and both in much the same way. Cloud forensics also faces many challenges associated with traditional digital forensics. Encryption and other anti-forensic techniques are commonly used in cloud-based crimes. The limited time for which forensically important data is available is also an issue with cloud-based systems. Because said systems are continuously running data, can be overwritten at any time. Time of acquisition has also proved to be a challenging task concerning cloud forensics (Lillis et al., 2016). Tracing the origin of malicious activities or devices within an IoT environment can be challenging without monitoring architecture with forensic logging capabilities. The key to improving research is the development and adoption of standards for case data, higher-level data abstractions, and implementable models for forensic processing (Garfinkel, 2010).

Blurry network boundaries and/or edgeless networks are an issue for IoT/IoA investigations i.e., without perimeter, or less clearly defined perimeters. The location of evidence effects ease of access, possible connection to other devices, local or cloud-based, etc. All available information on an IoT device can be recorded locally or in the cloud. Local storage is usually limited; thus, the number of recorded sensor values/actuator states is kept under a certain threshold and older data might not be accessible (Caviglione et al., 2017). Additionally, time synchronisation too is a key issue here. With multiple sources, they may present different time zone references, timestamp interpretations, clock skew/drift issues, and the syntax aspects involved in generating a unified timeline (Lillis et al., 2016). Legal and jurisdiction issues are commonplace; given the fact that some investigations encompass an international scope, e.g., data residing under multiple jurisdictions, laws and regulations must evolve to enable a global standard for digital forensics (Sachowski, 2016). The multi-jurisdictional, multi-environmental nature of cases results in different applications of digital forensic principles being seen by courts in different ways; therefore the methodology employed by digital forensic practitioners will always come under scrutiny (Adams, 2012).

Oriwoh et al. (Oriwoh et al., 2013) state any digital forensics solution that fails to consider the nature of the IoT to continually grow, adapt and mutate may eventually become too structured to be of any use. With an IoT-based environment, the networks bleed into each other with Body Area Networks (BAN) moving between Wide Area Networks (WAN) as people travel from, for instance, their homes to their places of work. One ramification for digital forensic investigators will be how to handle developing efficient methods of collecting all the relevant evidence from an object of forensic interest that has travelled between multiple networks, leaving multiple digital fingerprints in its wake. This is because in the IoT domain the boundaries between BAN, Personal Area Networks/Perimeter Area Networks/Premise Area Networks (PAN), Home Area Networks (HAN) or Hospital Area Networks (HAN), Local Area Networks (LAN), Neighbourhood Area Networks (NAN), Metropolitan Area Networks (MAN) and WAN will disappear and these networks will bleed into each other as users roam from one into another.

Figure 1 (Oriwoh et al., 2013) shows the movement of IoT-ware between inter-connected networks introduces challenges for digital forensics. IoT-based forensic solutions would have to recognise IoT-based devices as they approach and join networks, and recognise when they leave. Movement of things from one network to another can have implications for forensics because of the challenge of obtaining permission at the perimeters of these disparate networks as well as within the networks (Oriwoh et al., 2013).

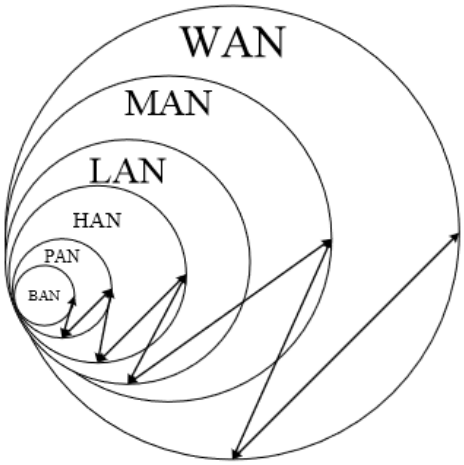

Figure 1. Movement of IoT-ware between inter-connected networks (Oriwoh, Jazani, Epiphaniou, & Sant, 2013)

Digital forensics will have to be able to investigate IoT components, which can range from nodes deployed in small scenarios (such as smart objects and smart watches) to those deployed in large ones (such as smart cities) – including analysis of attacks on IoT devices, and the digital forensics–aided investigations of physical-world crimes (Caviglione et al., 2017). Cloud forensics will also play a role in reinforcing cybersecurity best practices, since all data generated by IoT components will be stored on a cloud due to its scalability, capacity and convenience. Addressing security concerns will rely on a new era of digital forensics and best practices to simultaneously verify and leverage physical and digital evidence within a changing regulatory landscape (Salama, 2017). Movement of things from one network to another can have implications for forensics because of the challenge of obtaining permission at the perimeters of these disparate networks as well as within the networks.

A further challenge is that of available tools for digital forensic investigations. Increasingly investigators encounter data that cannot be analysed with today's tools because of format incompatibility, encryption, or the intricacy of the device. IoT forensics requires a multi-faceted approach where evidence may be collected from a variety of sources such as sensor devices, communication devices, cloud storage and ISP logs. Does the device hold data or is it simply middleware? For example, the Alexa enabled wireless smart speaker is a gateway for all voice commands submitted in the home. This intelligent virtual assistant interacts with a plethora of compatible IoT devices and third-party applications that leverages cloud resources (Chung, Park, & Lee, 2017). Understanding the complex cloud ecosystem that allows ubiquitous use of Alexa may be paramount for supporting IoT digital investigations in the future. Using innovative technologies, alongside the knowledge acquired from these studies as starting points for understanding the IoT world and IoT-ware will help in answering these questions and guiding more knowledge on IoT forensics. One of the major challenges to be addressed in the near future, is the creation of tools and techniques to analyse the bulk of data and report possible digital clues to the examiner for further investigation (Caviglione et al., 2017). While IoT data could be useful in investigations, the resulting clash with user privacy may lead to barriers in obtaining data and raise concerns about user data and privacy.

While cybercrime investigations and digital forensics have been affected by the identification, collection, and analysis of the vast amount of IoT devices available, there is a further challenge in the presentation of evidence. Data will often have undergone aggregation and processing using analytic functions that can

alter the structure and meaning of data. The granularity and semantics of evidence from the IoT will create challenges – at the device level, lossy compression techniques may reduce the granularity of the data to preserve limited resources such as memory, battery life, network bandwidth. (Hegarty, Lamb, & Attwood, 2014). As cloud and related technologies advance, forensic investigators will find it challenging to keep pace, in the sense of identifying new forensic artifacts. Thus, there is a need for ongoing research into identifying new forensic artefacts in the cloud and related environment (e.g. multi-cloud and federated cloud, fog computing, edge computing, and IoT), considering both data-at-rest and data-in-transit, as well as developing new forensically sound data collection techniques (Choo, Esposito, & Castiglione, 2017). To date, the digital investigation processes have been directed by technology being investigated and the available tools. Most of these procedures were developed for tackling different technology used in the inspected device. As a result, when underlying technology of the target device changes, new procedures have to be developed (Selamat, S. R., Yusof, R., & Sahib, 2008).

Without a clear strategy for enabling research efforts that build upon one another, forensic research will fall behind the market, tools will become increasingly obsolete, and law enforcement, military and other users of digital forensics products cannot rely on the results of forensic analysis (Garfinkel, 2010). Existing methodologies are designed for a different generation of evidence sources, and the assumption is that the objects of forensic interest will be available and accessible – while in the IoT, objects of forensics interest may not always be available or accessible. IoT usage creates a point of interaction between the cyber and physical worlds, making digital IoT forensics an effective way to collect information about the non-digital environment as well. Once the forensic investigators have located the suspected medium that has communicated with respected device, the forensic investigator could proceed with triage examination. During this period a very careful investigation is required as fragile data play a huge role in IoT forensic investigations. The most common device or platforms that need to cope with are router, gateway, Cloud platforms and Fog platforms. The collection of this device or platform also could be known as server cluster. The concept of IoT forensic in cloud and fog environment require a new mindset where some data will not be available, some data will be suspect, and some data will be court ready and can fit into the traditional network forensic mode (Perumal, Md Norwawi, & Raman, 2015).

CONCLUSION

Due to the tremendous influx of IoT-connected devices, it has become a necessity to develop a new process to investigate IoT-related incidents. Challenges for IoT-based forensic investigations include the increasing number of objects of forensic interest, relevance of identified and collected devices, blurry network boundaries, and edgeless networks. Containing an IoT breach is increasingly challenging – evidence is no longer restricted to a PC or mobile device, but can be found in vehicles, RFID cards, and smart devices. Addressing security concerns will rely on a new era of digital forensics and best practices to simultaneously verify and leverage physical and digital evidence within a changing regulatory landscape. While there are no defined principles for IoT forensics, investigations will significantly rely on the mechanical and physical nature of the smart device, since identifying evidence sources is a major challenge. Currently digital forensic and cyber security investigators are exploring the IoT concerning evidence handling, evidence extraction, and analysis of the collected data. Evidence can be collected from fixed sensors in homes and buildings, moving sensors built into cars and wearable devices, communication devices, cloud storage and even ISP logs. We expect that the practical study of this emerging field will identify methods for performing IoT-based digital forensics analysis. The study and presentation of considerations for the IoT/IoE area will lay a foundation for the forensic soundness and reliability of digital forensic processes in these future crime scenes.

REFERENCES

ACPO. (2012). ACPO Good Practice Guide for Digital Evidence. *Association of Chief Police Officers of England, Wales & Northern Ireland*, *5*(March), 41. Retrieved from http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf%0Ahttp://www.acpo.police.uk/documents/crime/2014/Revised Good Practice Guide for Digital Evidence_Vers 5_Oct 2011_Website.pdf

Adams, R. B. (2012). The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice. *Journal of Digital Forensics, Security and Law*, *8*(4), 1–254. Retrieved from http://researchrepository.murdoch.edu.au/14422/2/02Whole.pdf

Adams, R. B. (2013). *The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice.* Murdoch University. Retrieved from http://researchrepository.murdoch.edu.au/14422/2/02Whole.pdf

Al Fahdi, M., Clarke, N. L., & Furnell, S. M. (2013). Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. *2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference*, 1–8. http://doi.org/10.1109/ISSA.2013.6641058

Baker, T., Asim, M., Tawfik, H., Aldawsari, B., & Buyya, R. (2017). An energy-aware service composition algorithm for multiple cloud-based IoT applications. *Journal of Network and Computer Applications*, *89*(August 2016), 96–108. http://doi.org/10.1016/j.jnca.2017.03.008

Casciani, D. (2017). Cybercrime and fraud scale revealed in annual figures. Retrieved January 19, 2017, from http://www.bbc.co.uk/news/uk-38675683

Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. *IEEE Security Privacy*, *15*(6), 12–17. http://doi.org/10.1109/MSP.2017.4251117

Choo, K. K. R., Esposito, C., & Castiglione, A. (2017). Evidence and Forensics in the Cloud: Challenges and Future Research Directions. *IEEE Cloud Computing*, *4*(3), 14–19. http://doi.org/10.1109/MCC.2017.39

Chung, H., Park, J., & Lee, S. (2017). Digital forensic approaches for Amazon Alexa ecosystem. *Digital Investigation*, *22*, S15–S25. http://doi.org/10.1016/j.diin.2017.06.010

Corey, V., Peterman, C., Shearin, S., Greenberg, M. S., & Van Bokkelen, J. (2002). Network forensics analysis. *IEEE Internet Computing*, *6*(6), 60–66. http://doi.org/10.1109/MIC.2002.1067738

Dolliver, D. S., Collins, C., & Sams, B. (2017). Hybrid approaches to digital forensic investigations: A comparative analysis in an institutional context. *Digital Investigation*, *23*, 124–137. http://doi.org/10.1016/j.diin.2017.10.005

Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service., *arXiv prep*.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*, 64–73. http://doi.org/10.1016/j.diin.2010.05.009

Hausknecht, K., & Gruičić, S. (2017). Anti-computer forensics. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1233–1240).

Hegarty, R. C., Lamb, D. J., & Attwood, A. (2014). Digital Evidence Challenges in the Internet of Things. In *Proceedings of the Tenth International Network Conference (INC 2014)* (pp. 163–172).

Horsman, G. (2018). Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics. *Computers and Security*, *73*, 294–306. http://doi.org/10.1016/j.cose.2017.11.009

Khan, S., Gani, A., Wahab, A. W. A., Shiraz, M., & Ahmad, I. (2016). Network forensics: Review, taxonomy, and open challenges. *Journal of Network and Computer Applications*, *66*, 214–235. http://doi.org/10.1016/j.jnca.2016.03.005

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. http://doi.org/10.13140/RG.2.2.34898.76489

Liu, C., Singhal, A., & Wijesekera, D. (2017). Identifying Evidence for Cloud Forensic Analysis. In G. Peterson & S. Shenoi (Eds.), *Advances in Digital Forensics XIII* (pp. 111–130). Cham: Springer International Publishing.

Macdermott, Á., Baker, T., & Shi, Q. (2018). IoT Forensics: Challenges For The IoA Era. In *9th IFIP International Conference on New Technologies Mobility and Security (NTMS)* (pp. 1–5). Paris, France. http://doi.org/10.1109/NTMS.2018.8328748

Macdermott, Á., Shi, Q., & Kifayat, K. (2017). Distributed attack prevention using Dempster-Shafer theory of evidence. In Springer Verlag (Ed.), *ICIC 2017. Lecture Notes in Computer Science, vol 10363. In: Huang DS., Hussain A., Han K., Gromiha M. (eds) Intelligent Computing Methodologies.* (pp. 203–212). Springer, Cham.

McMurdie, C. (2016). The cybercrime landscape and our policing response. *Journal of Cyber Policy*, *1*, 85–93.

Mocas, S. (2004). Building theoretical underpinnings for digital forensics research. *Digital Investigation*, *1*(1), 61–68. http://doi.org/10.1016/j.diin.2003.12.004

Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of Things Forensics: Challenges and Approaches. *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*.

http://doi.org/10.4108/icst.collaboratecom.2013.254159

Perumal, S., Md Norwawi, N., & Raman, V. (2015). Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. *2015 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015*, 19–23. http://doi.org/10.1109/ICDIPC.2015.7323000

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, *1*(3), 1–12.

Rogers, M. (2003). The role of criminal profiling in the computer forensics process. *Computers & Security*, *22*(4), 292–298.

Rogers, M. (2006). DCSA: A Practical Approach to Digital Crime Scene Analysis. In *Information Security Management Handbook, 5th ed.* (pp. 601–614). New York, NY: Auerbach.

Sachowski, J. (2016). Understanding Digital Forensics. *Implementing Digital Forensic Readiness*, 3–16. http://doi.org/10.1016/B978-0-12-804454-4.00001-0

Salama, U. (2017). Smart Forensics for the Internet of Things (IoT). Retrieved March 22, 2017, from https://securityintelligence.com/smart-forensics-for-the-internet-of- things-iot/

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security*, *8*(10), 163–169.

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. *Computer Law & Security Review*, *26*(3), 304–308. http://doi.org/10.1016/j.clsr.2010.03.002