IoT Forensics: Challenges For The IoA Era

Áine MacDermott, Thar Baker, Qi Shi
Department of Computer Science,
Liverpool John Moores University,
Liverpool, UK
{a.m.macdermott; t.baker; q.shi}@ljmu.ac.uk

***Abstract*—Challenges for IoT-based forensic investigations include the increasing amount of objects of forensic interest, relevance of identified and collected devices, blurry network boundaries, and edgeless networks. As we look ahead to a world of expanding ubiquitous computing, the challenge of forensic processes such as data acquisition (logical and physical) and extraction and analysis of data grows in this space. 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. Through the combination of cloud-native forensics with client-side forensics (forensics for companion devices), we can study and develop the connection to support practical digital investigations and tackle emerging challenges in digital forensics. With the IoT bringing investigative complexity, this enhances challenges for the Internet of Anything (IoA) era. IoA brings anything and everything "online" in a connectedness that generates an explosion of connected devices, from fridges, cars and drones, to smart swarms, smart grids and intelligent buildings. Research to identify methods for performing IoT-based digital forensic analysis is essential. The long-term goal is the development of digital forensic standards that can be used as part of overall IoT and IoA security and aid IoT-based investigations.**

Keywords—computer forensics; mobile forensics; the Internet of Things; IoT; the Internet of Anything; IoA; forensic analysis; digital investigations.

I. Introduction

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. The increasing utilisation of cloud services in their day-to-day operations by organisations, 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 [1]. In the virtual environments provided in a cloud computing system, digital forensic investigations can prove quite troublesome due to the dynamic nature.

If a software application is accessed via a cloud computing system, data is traditionally written to the operating system (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 lost when the user exits the cloud. As identified by Taylor et al [3], virtualisation sanitises resources so the traditional analysis of leftover artefacts could be limited. This can make digital evidence traditionally stored on hard drives potentially unrecoverable [3]. While there are evident limitations with cloud-based forensic investigations, the increase in IoT-based devices increases this challenge with more complex investigative procedures required as individually and collectively, these devices produce, access and use large amounts of personal and sensitive data. On the one hand, finding potential evidence related to a crime is no more an issue due to availability of network logs, chat logs, emails and social networking posts. However, the challenge is to precisely analyse large volumes of data in timely manner and collect forensic evidence related to crimes being investigated, while detecting the presence of IoT activity. We do not anticipate the numbers of end nodes diminishing in the future, but rather expanding considerably and into the IoA era. Many of these devices are more vulnerable on networks due to their immature security capabilities, so we can be assured that investigations will be needed to understand what role these devices played in a breach. In addition, proprietary data formats, protocols, and physical interfaces all complicate the process of evidence extraction [4].

II. Background

The Internet of Things (IoT) is a concept coined to cover the interconnected infrastructure and utilities that are increasingly occurring. IoT is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure, from smart meters in homes, remote sensors for gas and oil utilities, interdependent system-of-systems: but the key issue is the fundamental problem with the interconnection of this "Internet of Things". The IoT is creating a wider attack surface, with billions of new and emerging devices. The IoT inherits the same monitoring requirements from cloud computing, however the related challenges are further affected by the characteristics of volume, variety, and velocity.

The IoT does not replace the existing ICT or operational technology networks; rather, it enhances these networks and relies on them in many ways. Recognising all these aspects working together, cyber security and physical security solutions must also work together with a coordinated focus on threats. With an estimated number of 50 billion devices that will be networked by 2020, specific attention must be paid to transportation, storage, access, and processing of the huge amount of data generated by these devices [2]. 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.

The IoT represents the seamless merging of the real and digital world, with new devices being created that store and pass around data. As a forensic analyst this creates problems, as we must find new ways to retrieve and secure this data making sure that there has been no tampering with the evidence. The purpose of this project is to find solutions to these problems by analysing how these different forms of evidence can be correctly seized, stored, extracted, and analysed. As of now, there is a standardised methodology for how to retrieve evidence from hard drives and mobile phones but no clear procedures for IoT-based investigations.

With the new types of devices that are part of the IoT, we must determine the best approach for ensuring they are examined in in the same forensically sound manner. As stated, the IoT is forever expanding; this paper will look forward at ways we can question and seize evidence from new devices, as they become part of the IoT, or the future IoA. For example, the Alexa [5] 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 [5]. 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.

III. The Changing Landscape of Crime

Developments and increased interconnection of us to the Internet, and devices to our everyday lives leads to the increases in cybercrimes. These developments and the anonymity that comes from the Internet serve as incentive to criminals and thus lead to an increase in crimes involving computers and cybernetics. Cybercrime is a broadly defined term and is often defined as "criminal activities carried out by means of computers or the Internet" [6] and is comprised of three main components:

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

There were an estimated 3.6 million cases of fraud and two million computer misuse offences in a year, according to an official survey by The Office for National Statistics [7]. Cybercrime is increasingly affecting a variety of domains: Government systems, large organisations, small to medium enterprises, ecommerce, online banking, and critical infrastructure. Motivations differ, but cybercrime for gain is significant, much more significant that 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, as well as effects to the confidentiality, integrity and availability of data.

Crime has always been a part of human society, but the means by which these crimes can be committed is 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, witnesses and interviews with suspects. Whereas today, the criminal investigator must recognise that the evidence they have to analyse could possibly be in an electronic or digital form. The crime scene may consist of a computer system or network as opposed to the traditional ‘physical’ scene.

A computer or its expanded peripherals do fall under the physical crime scene as they are a "physical" entity but obviously this expands into a digital crime scene. The ‘eye witness’ in these cases may be a computer generated log file. At a physical crime scene, the evidence may be in the form of latent fingerprints and impressions: Develop latent fingerprints; analyse and compare fingerprints, footwear and tire impressions; run fingerprints through IDENT1 for comparison against hundreds of millions of prints. In contrast, you can physically prove with science that someone was holding a certain weapon via DNA/fingerprints, but how do we prove that they were the one at the keyboard? As a computer forensic analyst, this would involve look at logs (such as emails, social media usage, web browser history, user accounts logged into the computer) – to prove that the user at the time was the one who committed the offence via factual evidence or behavioural profiling of usage.

Digital evidence can come in the form of many things. The main evidence would come from the hard drive of the criminals’ computer, laptop, external hard drives, USB devices, mobile devices, etc. There can be masses of data to analyse, as the amount of digital media and 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.

In order to deal with this fundamental change in evidence it is essential that the techniques used in these investigations must change and develop in order to deal with these effectively. As stated by Rogers, “*The science of digital forensics has developed, or more correctly is developing, while this science is arguably in its infancy, care must be taken to ensure that we do not lose sight of the goal of the investigative process, namely identifying the party or parties responsible*” [8]. While developing standards to deal with electronic or digital evidence, it is necessary that other supporting disciplines must also evolve in order to assist the investigator in this new realm and ensure they are knowledgeable on suitable conduct at the crime scene.

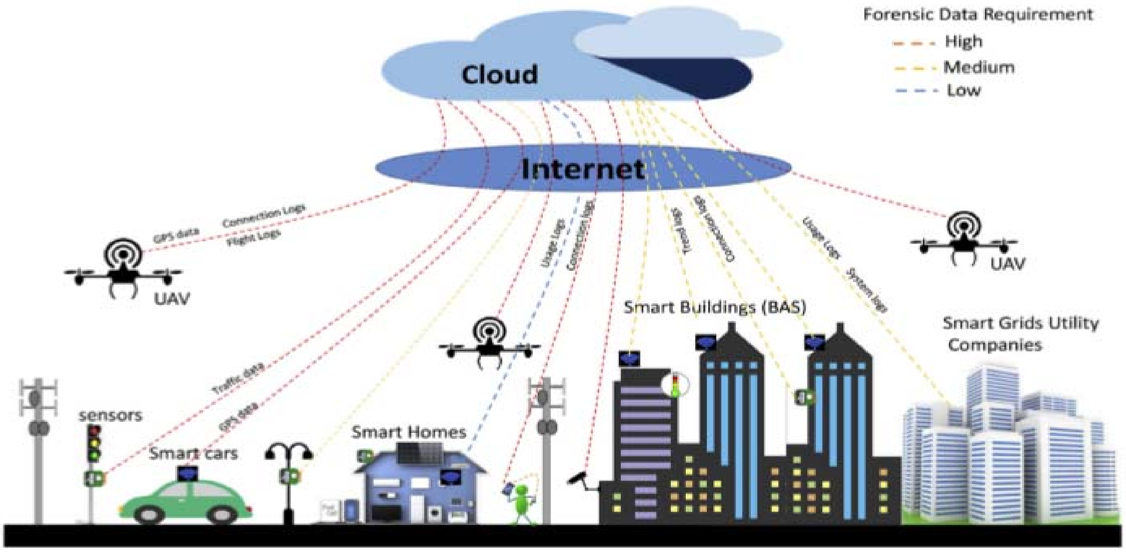

Fig. 1. Forensic data sources of the smart city illustrated with weight of evidence stored.

Recent work by Baig et al [9] took this issue a step further and examined the implications for smart cities with regards to cyber-security and digital forensics. Figure 1 [9] illustrates the forensic data sources in a smart city environment and the weight of evidence stored. The threats and criminal misuses in a smart city are increasingly heterogeneous and significant, with provisioning of resilient and end-to-end security being a daunting task. When a cyber-incident involving critical components of the smart city infrastructure occurs, appropriate measures can be taken to identify and enumerate concrete evidence to facilitate the forensic investigation process.

IV. Forensic Evidence Handling

A. *Forensic Methodologies*

A digital forensics methodology provides a framework for procedures and processes that should be followed when engaging in a digital forensic based investigation. There is no standardised methodology to follow at a crime scene and the use is dependent upon the investigator. There are many to choose from, each comprise the same main stages (secure, analyse, present), but with differing attention focusing on different stages. For example, the Advanced Data Acquisition Model (ADAM) methodology [10] allocates considerable time for pre-planning and pre-investigative stages, whereas 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) [11].

Forensic computer analysts identity all of the computer equipment, tag items of importance and take them back to the computer labs for analysis. They also photograph the scene in order to ensure things are put back correctly. In handling evidence it is always important to follow the three C's of evidence: care, control and chain of custody. By following this process it ensures that the evidence seized is the same as the evidence that may be presented in court. They also need to maintain chain of custody during the documentation of evidence, as documenting a case in a fact-based manner is essential to the integrity of it.

Forensic computer analysts scrutinize seized data and explain the current state of the digital artefact. Computer forensic investigations usually 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. Typical forensic analysis includes a manual review of the material on the media, namely analysing documents, images, emails, etc.; and highlighting files of suspicion. Reviewing the Registry for suspicious information is an additional action, as is using keyword searches for topics related to the offence in the hope that files of suspicion are found – which is a quite lengthy and time consuming process.

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. Indeed, any investigation within the public or private arena is likely to involve the seizure, preservation and examination of electronic evidence, therefore a digital evidence strategy must form an integral part of the wider investigative process [12].

It is clear that the current actions undertaken by investigators, regardless of forensics methodology followed, are underpinned by the ACPO (Association of Chief Police Officers) guide. 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 different 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 matter.

The ACPO guide lists principles for computer-based electronic evidence and is listed below [13]:

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 good chain of custody. Currently computer forensic and cyber security experts are exploring the IoT from the perspective of a computer forensic analyst with regards to evidence handling, evidence extraction, and analysis of the collected data. There are many questions that remain to be answered in this emerging area. 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 the industry with more knowledge on IoT forensics.

B. *Time for change*

Science has been involved in criminal investigations for a long time and it has developed alongside the nature of the crimes. The field of digital evidence is unlike most other forensic sciences as the nature of the material under examination is determined, largely by human ingenuity. Rather than looking for traces of material deposited by physical or biological entities, which tend to develop and evolve slowly, we deal with technology, which is updated, enhanced and even created at an alarming rate [14]. In order 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, analyse the evidence, and identify 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 in order to assist the investigator [15]. There are no defined principles for IoT forensics, as such, investigations will significantly rely on the mechanical and physical nature of the smart device, since identifying evidence sources is a major challenge. Evidence could 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.

The main challenges posed by an IoT-based crime scene from the perspective of an investigator include:

- Size of objects of forensic interest;
- Location - effects ease of access, possible connection to other devices, local or cloud-based, etc.
- Relevance of identified and collected devices;
- Legal/Jurisdiction issues;
- Blurry network boundaries/ Edgeless networks i.e. no perimeter, or less clearly-defined perimeters.
- Available tools – adequate for tasks? Is the data encrypted? Does the device hold data or is it simply middleware?

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 – whereas in the IoT, objects of forensics interest may not always be available or accessible [16]. Cloud forensics will also play a main role in reinforcing cybersecurity best practices, since all data generated by IoT components will be stored on cloud due to its scalability, capacity and convenience. As a result of the continued growth in the number of IoT-connected devices, it has become a necessity to develop a new process to investigate IoT-related incidents. 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 [17].

V. Internet of Anything (IoA)

Taken to extremes, the IoA subsumes drones, smart swarms, the smart grid, intelligent buildings, and autonomous cyber-physical and cyber-biological systems, each of which has achieved or is about to achieve mega-cliché status on its own merit. The IoA is supported by the cloud, big data, mobile computing, and bring your own device (BYOD). While, the IoT bringing investigative complexity, this enhances challenges for the IoA era. The IoA brings anything and everything "*online*" in a connectedness that generates an explosion of connected devices, from fridges, cars and drones, to smart swarms, smart grids and intelligent buildings. Research to identify methods for performing IoT-based digital forensic analysis is essential. Mackay et al. [18] and Baker et al. [19] present a set of essential security services, embedded within a cloud-based "*Security Toolbox*", including end-to-end security services (e.g., secure virtualisation, and encrypted file system), service planning (e.g., Trust-based cloud, and SLA negotiation), and monitoring and policing (e.g., dynamic cloud monitoring and user access control). It should be noted that the toolbox and the associated services are developed in the context of a centralised SOA-based SCADA systems platform for critical infrastructures, in which none of the services were designed to help in data acquisition for forensic purposes. Thus, the long-term goal of this work is the development of digital forensic standards, tools and services that can be used as part of overall IoT/IoA security.

Sources of evidence on IoT-based devices can be categorised into three groups [17]:

- All evidence collected from smart devices and sensors;
- All evidence collected from hardware and software that provide a communication between smart devices and the external world (e.g., computers, mobile, IPS, IDS and firewalls), which are included in traditional computer forensics; and
- All evidence collected from hardware and software that are outside the network under investigation. This group includes cloud, social networks, ISPs and mobile network providers, virtual online identities and the Internet.

The main IoT/IoA challenge from a forensic perspective is that of data acquisition – knowing exactly where the data is and actually acquiring the data. The search and seizure procedures used in the conventional computer forensic process are impractical due to evidence being stored in cloud datacenters. It is also difficult if not impossible to maintain a 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 ACPO principles [13].

In addition, cloud cybersecurity policies will require revision, as each IoT device generates data that is stored in the cloud. Cloud cybersecurity policies should be integrated with IoT infrastructure to have quick responses for any suspicious activity. The policy should be revised in terms of evidence identification, data integrity, preservation, and accessibility. Cloud service providers should ensure the integrity of the digital evidence retrieved from cloud computing components to have a fair investigation process in identifying the root cause of the attack in IoT [20]. 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.

VI. Conclusion

As a result of the continued growth in the number of IoT-connected devices, it has become a necessity to develop a new process to investigate IoT-related incidents. 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 computer forensic and cyber security investigators are exploring the IoT from the perspective of a computer forensic analyst with regards to evidence handling, evidence extraction, and analysis of the collected data. Evidence could 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. There are many questions that remain to be answered in this emerging area, which could enhance the overall curriculum going forward. We anticipate that the practical study of this emerging field will identify methods for performing IoT-based digital forensic analysis.

References

[1] M. Taylor, J. Haggerty, D. Gresty, and R. Hegarty, “Digital evidence in cloud computing systems,” Computer Law & Security Review, vol. 26, no. 3, pp. 304–308, 2010.

[2] A. Botta, W. Donato, V. Perisco et al., “On the Integration of Cloud Computing and Internet of Things,” in *International Conference on Future Internet of Things and Cloud (FiCloud),* 2014, pp. 23-30.

[3] M. Taylor, J. Haggerty, D. Gresty, and D. Lamb, “Frensic investigation of cloud computing systems,” Network Security, vol. 2011, no. 3, pp.4-10, March 2011.

[4] R. C. Hegarty, D. J. Lamb, and A. Attwood, “Digital Evidence Challenges in the Internet of Things,” in *Proceeding of the Tenth International Conference (INC 2014)*, 2014, pp. 163-172.

[5] H. Chung, J. Park, and S. Lee, “Digital forenisc approaches for Amazon Alexa ecosystem,” *Digital Investigations*, vol. 22, pp15-35, 2017.

[6] C. McMurdie, “The cybercrime landscape and our policing response”, in *Journal of Cyber Policy*, vol. 1, no. 1, pp.85-93.

[7] BBC, “Cybercrime and fraud scale revealed in annual figures”, 19th January 2017, http://www.bbc.co.uk/news/uk-38675683.

[8] M. Rogers, “The role of criminal profiling in the computer forensics process”, in *Center for Education and Research in Information Assurance and Security*, 2003, pp. 292-298.

[9] Z.A., Baig, et al. “Future challenges for smart cities: Cyber-security and digital forensics”. Digital Investigation, volume 22, pp.3-13, 2017.

[10] Adams, R., Hobbs, V., Mann, G.: The advanced data acquisition model (ADAM): a process model for digital forensic practice. Journal of Digital Forensics, Security and Law, 8(4), 25–48 (2014).

[11] G. Mohay, A. Anderson, B. Collie, O. de Vel and R. McKemmish, Computer and Intrusion Forensics, Artech House, Norwood, Massachusetts, 2003.

[12] 7Safe, “Good Practice Guide for Computer-Based Electronic Evidence”, https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence%5b1%5d.pdf

[13] Association of Chief Police Officers of England, Wales & Northern Ireland, “ACPO Good Practice Guide for Digital Evidence,” http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[14] A. Marshall, “Digital forensics, digital evidence in criminal investigation”, Wiley-Blackwell, 2008.

[15] M. Rogers, “The role of criminal profiling in the computer forensics process”, in *Computers & Security*, 2003, vol. 22, issue 4, pp.292-298.

[16] J. Liu, “IoT Forensics: Issues, Strategies, and Challenges”, at 12th IDF Annual Conference, 15th December 2015, https://digitalforensic.jp/wp-content/uploads/2016/03/community-12-2015-07.pdf

[17] U. Salama, “Smart Forensics for the Internet of Things (IoT)”, Security Intelligence IBM, 22nd March 2017, https://securityintelligence.com/smart-forensics-for-the-internet-of-things-iot/

[18] M. Mackay, T. Baker, A. Al-Yasiri, “Security-oriented Cloud Computing Platform for Critical Infrastructure”, Journal of Computer Law and Security, 28, no. 6, pp. 679-686, 2012.

[19] T. Baker, M. Mackay, A. Shaheed, B. Aldawsari, “Security-oriented Cloud Platform for SOA-based Scada”, in the proceeding of the 15th IEEE/ACM international conference on Cluster, Cloud and Grid Computing (CCGrid), 2015.

[20] S. Khan, “The Role of Forensics in the Internet of Things: Motivations and Requirements”, in IEEE Internet Initiative eNewsletter, July 2017.