The Internet of Things: Challenges and Considerations for Cybercrime Investigations and Digital Forensics

Áine MacDermott, Liverpool John Moores University, Merseyside, UK

Thar Baker, Liverpool John Moores University, Merseyside, UK

https://orcid.org/0000-0002-5166-4873

Paul Buck, Liverpool John Moores University, Merseyside, UK

Farkhund Iqbal, Zayed University, Abu Dhabi, UAE

Qi Shi, Liverpool John Moores University, Merseyside, UK

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 with 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 article 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, Cybercrime Investigations, Digital Forensics, Forensic Analysis, Internet Of Anything, Internet Of Everything, Internet Of Things, IoT, Mobile 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

DOI: 10.4018/IJDCF.2020010101

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.

Related Content