


# Digital Forensics: Challenges and Opportunities for Future Studies

Reza Montasari, University of Huddersfield, Huddersfield, UK


Richard Hill, University of Huddersfield, Huddersfield, UK

Simon Parkinson, University of Huddersfield, Huddersfield, UK

 <https://orcid.org/0000-0002-1747-9914>

Pekka Peltola, CAR-CSIC, Center of Automation and Robotics, Spanish Research Council, Madrid, Spain

Amin Hosseinian-Far, University of Northampton, Northampton, UK

 <https://orcid.org/0000-0002-2534-9044>

Alireza Daneshkhah, Coventry University, Coventry, UK

## ABSTRACT

Considering the ever-growing ubiquity of technology, there is an associated growth in the possibility of digital devices related to a criminal investigation or civil litigation. As the variety of digital devices is increasing, the storage capacity of each is also rising exponentially. Due to the varied and large volumes of data produced, law enforcement agencies (LEAs) worldwide are facing a significant backlog of cases. This has culminated in significant delays in dealing with cases that urgently require digital forensic investigations (DFIs). It is of paramount importance that new research approaches be adopted to address such challenges. This article evaluates the existing set of circumstances surrounding the field of digital forensics (DF). The article provides two important contributions to the field of DF; it identifies and analyses the most important mid- and long-term challenges that need to be considered by LEAs. It also proposes important specific future research directions, the undertaking of which can assist LEAs in adopting a new approach to addressing these challenges.

## KEYWORDS

Digital Forensics, Digital Investigation, Big Data, IoT Forensics, Cloud Forensics, Cybersecurity, Encryption

## 1. INTRODUCTION

Over the past few years, technology has become prevalent in many aspects of day to day life. we have witnessed rapid advancements in Information and Communication Technology (ICT) features. Technologies such as communication networks, mobile devices, Internet of Things (IoT) solutions, Cloud-Based Services (CBSs), Cyber-Physical Systems (CPSs) have brought many benefits to technologically advanced societies (Montasari & Hill, 2019; Montasari, 2017b; Caviglione et al., 2017; Pichan et al., 2015). As a result, commercial transactions and governmental services have rapidly grown, revolutionising the lifestyles of many individuals living in these societies. While technological advancements undoubtedly present many advantages, at the same time they pose new cybersecurity threats (Jahankhani et al., 2014), which have significant impacts on a variety of domains such as government systems, enterprises, ecommerce, online banking, and critical infrastructure

DOI: 10.4018/IJOI.2020040103

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

(Hosseini-Far et al., 2017). According to an official survey conducted by The Office for National Statistics (BBC, 2017), there were an estimated 3.6 million cases of fraud and two million computer misuse offences in a year.

Some of the challenges resulting from such technological advancements include, but are not limited to: high volume of data, heterogeneous nature of digital devices, advanced hardware and software technologies, anti-forensic techniques, video and rich media, whole drive encryption, wireless, virtualisation, live response, distributed evidence, borderless cybercrime and dark web tools, lack of standardised tools and methods, usability and visualisation. The deployment of IP anonymity and the ease with which individuals can sign up for a cloud service with minimum information can also pose significant challenges in relation to identifying a perpetrator (Caviglione et al., 2017; Lillis et al., 2016; Chen et al., 2012; Ruan et al., 2011; Cameron, 2018). As a result, the number of cases that necessitate DFIs are on the rise, culminating in the creation of a backlog of cases for LEAs worldwide (Montasari, 2016a; Montasari, 2016c). Without a clear plan to facilitate research efforts that extend one another, forensic research will lag behind, tools will become outdated, and law enforcements' products will be incapable of relying on the results of DF analysis (Garfinkel, 2010; Montasari et al., 2019).

In recent years the area of digital forensics has attracted interest from researchers, with notable survey and position papers being published. One recent position paper (Watson & Dehghantanha, 2016) states the high-level challenges associated with performing digital forensics on IoT devices. The authors focus their attention on the location and inability to extract meaningful data from IoT devices. However, they provide little information on what the future direction of this field might be, which could for example, include IoT producers accommodating forensic capabilities from the design stage of the technology. In another study, the authors focus their attention on suggesting future challenges within Smart Infrastructure, which includes IoT devices (Baig et al., 2017). IoT forensic can be related to data, service and/or architecture fusion. Sometimes fusion with other data and users is common. Innovative solutions/recommendations are required to resolve some of the known existing issues (Kuo et al., 2018). The paper provides a comprehensive speculation as to the threats facing Smart Infrastructure and how digital forensics might be performed.

A widely cited key survey published in 2010 (Garfinkel, 2010) provides future paradigms of research, and although relevant, changing IT patterns have resulted in the need for this subject to be revised. For example, in the position paper, future research directions are presented and justified. These areas are: 1) modulization; 2) alternative analysis mechanisms; 3) scale and validation; 4) abstraction. Directions 1, 2, and 3 have demonstrated to be true and areas of continuing research; however, direction 4 (abstraction) is somewhat understated and premature to the needs of current digital forensics. Although, there is clearly a need to abstract the forensic challenge and make it easier, quicker and more reliable for the investigator, the introduction of IoT devices has resulted in the absence of low-level techniques and processes for forensic acquisition. This therefore motivates the perusal of IoT forensics is a precursor to abstraction.

Therefore, in light of the discussion above, it is of paramount importance that new research approaches be undertaken to address the aforementioned challenges. To this end, we evaluate the existing set of circumstances surrounding the field of DF. Our research study makes two important contributions to the field of DF. First, it analyses the most difficult mid and long-term challenges that need to be considered by LEAs. Second, it proposes important specific future research directions, the undertaking of which can assist LEAs in adopting a new approach to addressing such challenges.

## 2. CHALLENGES

The current states of DF encounters numerous challenges, from both ethical and technological perspectives. As the field of DF continues to evolve, its development is severely challenged by the growing popularity of digital devices and the heterogeneous hardware and software platforms being utilised (Caviglione et al., 2017). For instance, the increasing variety of file formats and OSs hampers

the development of standardised DF tools and processes (Montasari & Hill, 2019). Furthermore, the emergence of smartphones that increasingly utilise encryption renders the acquisition of digital evidence an intricate task. Khan et al. (2016) conducted a deep SWOT analysis for all IoT forensic adoption, cases, services with a view to enhance awareness of challenges and situations for businesses and all stakeholders involved. IoT forensic and privacy assessment is of a great importance in certain industries in which sensitive data are being handled. An instance of such industries includes healthcare; Yang et al. (2019) have proposed solutions to address some of such challenges.

## 2.1. Cloud Forensics

In all circumstances implicating cloud service and deployment models, the cloud customer encounters issues in relation to decreased access to forensic data based on the cloud model that is implemented (Baig et al., 2017; Chen et al., 2012). For instance, IaaS users might enjoy relatively easy access to all data needed for forensic investigation, whereas SaaS customers might have little or no access to such data (Jahankhani & Hosseinian-Far, 2015). Lack of access to forensic data denotes that the cloud customers will have little control (or no control) or even knowledge of where their data is physically located. Cloud customers might only be able to specify the location of their data at a higher level of abstraction, typically as a virtual object container. This is due to the fact that CLSs deliberately hide the actual location of data in order to assist data movement and replication (Lukan, 2014). Moreover, there is a lack of the terms of use in the Service Level Agreements in order to facilitate forensic readiness in the cloud. Many CSPs purposely avoid offering services or interfaces that will assist customers in collecting forensic data in the cloud. For example, SaaS providers do not provide IP logs or clients accessing content, while IaaS providers do provide copies of recent Virtual Machine states and disk images. The cloud as it operates now does not offer customers with access to all the relevant log files and metadata and limits their ability to audit the operations of the network utilised by their provider and conduct real time monitoring on their own networks.

In relation to the static and live forensics within the cloud, the propagation of endpoint, particularly mobile endpoints, is one of the major challenges for data discovery and evidence acquisition. The large number of resources connected to the cloud makes the impact of crimes and the workload of investigation even larger (Ruan et al., 2011). Constructing the timeline of an event needs accurate time synchronization which is vital in relation to the audit logs employed as source of evidence in the investigations (Jahankhani & Hosseinian-Far, 2015). Accurate time synchronization is one of the major issues during network forensics, and it is often aggravated by the fact that a cloud environment needs to synchronize timestamps that is in harmony with different devices within different time zones, between equipment, and remote web clients that include numerous end points. The usage of disparate log formats is already an issue in traditional network forensics. The issue is aggravated in the cloud because of the large volume of data logs and the pervasiveness of proprietary log formats. Researchers are developing mechanisms to automatically establish knowledge from event logs, including the use of machine learning techniques to establish correlation (Parkinson et al., 2017). However, key challenges exist in the scalability of such techniques to the large amounts of data generated. For example, one commercial IT infrastructure can generate billion of events per 24-hour period.

Analogous to other branches of forensics, deleted data in the cloud is considered as a vital piece of artefact. The customer who created a data volume often maintains the right to modify and remove the data. When the customer removes a data item, the deletion of the mapping in the domain begins immediately and is typically completed in seconds (Ruan et al., 2011; Cameron, 2018). After that, there is no way to access the removed data remotely, and the storage space, having been occupied by the said data, becomes available for future write operations, and it is possible that the storage space will be overwritten by newly stored data. However, some removed data might still be present in a memory snapshot. Therefore, the challenge is to recover the deleted data, identify the ownership of the deleted data, and employ the deleted data for event reconstruction purposes in the cloud.

Concerning evidence segregation in the cloud, the various instances of virtual machines running on the same physical machine are isolated from each other via virtualization. The instances are treated as if they were on separate physical hosts, and as such, they will have no access to each other despite being hosted on the same machine (CSA, 2009). Customer instances do not have access to raw disk devices, instead they have access to virtualized disks. Technologies employed for provisioning and deprovisioning resources are constantly being updated (Jahankhani & Hosseinian-Far, 2015; CSA, 2009). CSPs and law enforcement agencies often face a challenge to segregate resources during investigations without violating the confidentiality of other tenants that share the same physical hardware, while also ensuring the admissibility of the evidence (Lukan, 2014). Another challenge is that the easy-to-use feature of cloud models facilitates a weak registration system. This makes anonymity easier which enables cybercriminals to hide their identities and more difficult for investigators to detect and trace perpetrators. CSPs employ encryption in order to segregate data between cloud customers. However, when this feature is not available, customers are often encouraged to encrypt their sensitive data before uploading it to the cloud (Ruan et al., 2011). Therefore, it is suggested that the segregation must be standardized in SLAs and access to cryptographic keys must also be formalized consistent with CSPs, consumers and law enforcement agencies.

Furthermore, virtualisation within the cloud environments poses several challenges. For instance, malware and hacker attacks have a growing impact on virtualised systems. Moreover, cloud computing provides data and computing power redundancy by duplicating and distributing resources. Many CSPs do this by employing different instances of a cloud computer environment within a virtualized environment, with each instance running as a stand-alone virtual machine that is monitored and maintained by a hypervisor (Jahankhani & Hosseinian-Far, 2015). This denotes that attackers can target the hypervisor and doing so successfully provides them with free control over all the machines being managed by it. However, at the same time, there is a lack of policies, techniques, and procedures on the hypervisor level that could assist CFIs in conducting cloud forensic investigations. Another challenge presented is the loss of data control. Data mirroring over multiple machines in various jurisdictions and the lack of clear, real-time information about data locations presents challenges in forensic investigations (Catteddu, 2010). Moreover, a CSP cannot offer an exact physical location for a piece of data across all the geographical regions of the cloud. Also, the distributed nature of cloud computing necessitates robust international cooperation, particularly when the cloud resources to be seized are located around the world (Ruan et al., 2011; Lukan, 2014).

## **2.2. Internet of Things (IoT) Forensics**

Despite its many benefits, IoT-connected devices pose significant privacy and security challenges as these devices and systems collect significant personal data about individuals. As an example of privacy challenge, employers can use their employees' security access cards to track where they are in the building to determine how much time the employees spend in their office or in the kitchen. Another example relates to smart meters that can determine when one is home and what electronics they use. This data is shared with other devices and stored in databases by companies. Other instances of IoT technology areas that pose challenges to forensic investigators include wearables, UAVs, prototyping microcontrollers, medical devices, sensor networks, home automation, smart vehicles, 3D printers, connected appliances, security systems, access control systems, mobile phones and sensor network technologies (Watson & Dehghantanha, 2016).

A recent survey of security challenges facing connected and autonomous vehicles highlighted forensics for the purposes of insurance to be a key challenge for the industry (Parkinson et al., 2017). For example, vehicle data can be used to determine driver fault in accidents, through gaining a comprehensive analysis of what both driver and vehicle were doing at the time. Furthermore, the survey also highlighted that vehicles forensics will be necessary in understanding accidents that occur involve entirely autonomous vehicles. One paper performs an analysis as to the variety of information available within vehicles, demonstrating the potential for its use in forensics. The vehicle

industry has recognised the necessity of vehicle forensics; however, due to the complexity of their software systems, it is widely attributed to requiring significant research and investment. Current literature exists providing frameworks for performing analysis, as well as studies focussed on specific challenges; however, due to the rapid technological developments in the field, it requires continuous updating (Parkinson et al., 2017).

The challenges facing vehicle forensics are ubiquitous with those of IoT challenges, and although IoT uses the same monitoring requirements similar to those utilised by cloud computing, it produces a wider security attack surface than that created by cloud computing. Examples of cyberattacks that can be carried out on IoT devices include: intercepting and hacking into cardiac devices such as pacemakers and patient monitoring systems, launching DDoS attacks using compromised IoT devices, hacking or intercepting In-Vehicle Infotainment (IVI) systems, and hacking various CCTV and IP cameras. It poses more security challenges resulting from issues such as volume, variety and velocity. Furthermore, DFIs of IoT devices can be even more difficult than those of cloud-based investigations due to the constant emergence of new and diverse devices with varied OSs as well as the different networks and related protocols. As a result, more complex procedures are needed for investigation of these devices.

IoT Forensics must involve identification and extraction of evidential artefacts from smart devices and sensors, hardware and software which facilitate a communication between smart devices and the external world (such as computers, mobile, IPS, IDS and firewalls), and also hardware and software which are outside of the network being investigated (such as cloud, social networks, ISPs and mobile network providers, virtual online identities and the Internet). However, extracting evidential artefacts from IoT devices in a forensically-sound manner and then analysing them tend to be a complex process, if not impossible, from a DF perspective. This is due to a variety of reasons, including: the different proprietary hardware and software, data formats, protocols and physical interfaces, spread of data across multiple devices and platforms, change, modification, loss and overwriting of data, and jurisdiction and SLA (when data is stored in a cloud).

Thus, determining where data resides and how to acquire data can pose many challenges to DFEs. For instance, the DF analysis of IoT devices used in a business or home environment can be challenging in relation to establishing whom data belongs to since digital artefacts might be shared or transmitted across multiple devices. In addition, due to the fact that IoT devices utilise proprietary formats for data and communication protocols, understanding the links between artifacts in both time and space can be very complex. Another challenge related to the DFI of IoT devices concerns the chain of custody. In civil or criminal trial, collecting evidence in a forensically sound manner and preserving chain of custody are of paramount importance (Montasari, 2017c; Montasari et al., 2019; Montasari et al., 2019; Montasari, 2018; Montasari, 2017a; Montasari, 2016e). However, ownership and preservation of evidence in an IoT setting could be difficult and can have a negative effect on a court's understanding that the evidence acquired is reliable.

Furthermore, existing DF tools and methods used to investigate IoT devices are designed mainly for traditional DF examining conventional computing devices such as PCs, laptops and other storage media and their networks. For instance, the current methods utilised to extract data from IoT devices include: obtaining a flash memory image, acquiring a memory dump through Linux dd command or netcat, and extracting firmware data via JTAG and UART techniques. Moreover, protocols such as Telnet, SSH, Bluetooth and Wi-Fi are deployed to access and interact with IoT devices. Likewise, tools such as FTK, EnCase, Cellebrite, X-Ways Forensic and WinHex, etc. and internal utilities such as Linux dd command (for IoT devices with OSs such as embedded Linux) are used to extract and analyse data from IoT devices. However, the forensic investigation of IoT devices necessitates specialised handling procedures, techniques, and understanding of various OSs and file systems. Additionally, by using conventional Computer Forensic tools to conduct IoT Forensics, it would be highly unlikely to maintain a chain of custody, the adherence to which is required by the Association of Chief Police Officers (ACPO, 2012; Montasari et al., 2015), concerning the collection of digital evidence.

Another forensic challenge encountered by DFPs relates to the file systems of IoT devices. In a typical DF context, DFPs often run into computer and mobile device OSs with a known set of file systems. However, IoT devices come with different types of file systems which are often unknown to DFPs. This is while there are very few forensic tools available to DFPs for parsing and extracting data from these devices. Examples of IoT device hacking can include: interception of cardiac devices (such as pacemakers, Patient/Infant monitoring systems), launching DDOS attacks using compromised IoT devices, hacking into In-Vehicle Infotainment (IVI) systems, hacking into various CCTV and IP cameras. Compared to the standard DF acquisition and analysis techniques, IoT Forensics poses significant challenges due to the heterogenous and complex nature of IoT devices and IoT Ware, proprietary software and hardware, data being spread across multiple devices and platforms, data being changed, modified, and lost/overwritten quickly, and also jurisdiction and SLA constraints when data is stored in a cloud or a different geographic location. Although in theory, IoT Forensics is not different from standard DF principles and processes, it necessitates a distinct handling procedures, techniques, and knowledge of multiple OSs and file systems.

Other forensic challenges posed by IoT devices include issues such as availability, authenticity and non-repudiation which are essential for forensically sound used of data (Lillis et al., 2016). Persistency of data is also another challenge posed by IoT devices which tend to have limited memory or no persistent data storage. Consequently, any data stored for longer periods is likely to be stored in in-network hubs or to be transferred to the cloud for more persistent storage. As a result, problems associated with Cloud Forensics (as discussed in Sub-Section 2.1) will also be relevant to the field of IoT. Although over the past few years, the research community have been examining IoT devices for the purposes of forensics, these works are still in their infancy. Therefore, in order to keep pace with the new IoT devices, IoT Forensics requires a multi-faceted approach in which evidence can be collected and analysed from a variety of sources such as sensor devices, communication devices and cloud storage, etc.

### **2.3. Big Data and Backlog of Digital Forensic Cases**

Another key challenge that the field of DF is currently facing pertains to the substantial and continuing increase in the amount of data, i.e. big data – both structured and unstructured – acquired, stored and presented for forensic examination. This data is collected from a variety of sources such as common and uncommon locations in digital devices (Montasari & Peltola, 2015), networks, cloud, IoT devices, social media, sensors or machine-to-machine data, etc. In particular, this challenge is relevant to live network analysis since DFEs are unlikely to acquire and store all the essential network traffic (Caviglione et al., 2017; Cameron, 2018). This growth in data volume is the consequence of the ongoing advancement of storage technology such as growing storage capacity in devices and cloud storage services, and an increase in the number of devices seized per case. Consequently, this has resulted in an increase in the backlog of DF cases that are awaiting (often many months or years in some cases) investigations. The backlog of DF cases necessitating investigation has had a seriously adverse impact on the timeliness of criminal investigations and the legal process. The delays of up to 4 years in performing DFIs on seized digital devices have been reported to have significant effect on the timeliness of criminal investigations (Lillis et al., 2016; Montasari, 2016a; Quick & Choo, 2014). Due to such delays, some prosecutions have even been discharged in courts. This backlog of DF cases is predicted to increase due to the modern sources of evidence such as those of IoT devices and CBSs.

To address the aforementioned issues, i.e. the 3Vs of the big data, including: volume, variety and velocity, researchers have, in recent years, proposed various solutions ranging from data mining, data reduction and deduplication (Quick & Choo, 2014; Beebe & Clark, 2005; Palmer, 2001; Farsi et al., 2019), triage (Montasari, 2016c; Garfinkel, 2010; Mislan et al., 2010; Casey et al., 2009), increased processing power, distributed processing (Roussev & Richard, 2004), cross-drive analysis (Palmer, 2001), artificial intelligence, and other advanced methods (Beebe & Clark, 2005). Despite the usefulness of these solutions, additional research studies are required to address the real-world

relevance of the proposed methods to deal with the data volume that gravely challenges the field of DF. Therefore, it is of paramount importance to implement several practical infrastructural enhancements to the existing DF process. These augmentations should cover elements such as automation of device collection and examination, hardware-facilitated heterogeneous evidence processing, data visualisation, multi-device evidence and timeline resolution, data deduplication for storage and acquisition purposes, parallel or distributed investigations and process optimisation of existing techniques. Such enhancements should be integrated to assist both law enforcement and third-party providers of DF service to speed up the existing DF process. The implementation of the stated elements can significantly assist both new and augmented forensic processes.

## **2.4. File System and Encryption**

It is challenging, if not impossible, to acquire data from encrypted devices. Although encryption is not unbeatable, it necessitates large amount of time, skills and resources to be bypassed. A growing number of OSs facilitates the encryption of the file system. Despite the fact that this provides the legitimate end users with additional security and privacy, at the same time it poses significant challenges to DFPs. The extent of encrypted file systems is predicted to grow to the degree that they will ultimately become the default approach in future implementations. Furthermore, in order to conduct forensically sound investigations and preserve the integrity of digital device that has been seized for forensic acquisition and analysis, DFPs are required to access the device using a write-blocker and use forensic tools (such as FTK, EnCase or Cellebrite, etc.) to create forensic images. This forensic image is then utilised to examine files, installed applications, slack and unallocated space, and swap files, etc. to search for fragments of data. However, the growing number of digital devices used in a crime and the volume of data render the imaging and the examination of the image exceedingly time-consuming. Furthermore, considering that disk drives are increasingly becoming larger in data storage capacity, it takes longer to acquire them for subsequent forensic analysis. For instance, imaging a 1TB hard disk (HDD) can take approximately 20 hours. As a result, there is often inadequate time to create a forensic image of the suspect digital device or to analyse all of the data once it is discovered. Furthermore, DFPs can no longer remove or image storage devices easily because of the growing propagation of embedded storage and the prevalence of hardware interfaces (Garfinkel, 2010). The plethora of different types of operating systems and file formats increases the requirements and intricacy of data manipulation tools and the cost of tool development. Prevalence in data encryption prevents DFPs from being able to process data even when they are able to recover it (Garfinkel, 2010; Casey & Stellatos, 2008). Cloud data cannot be readily recovered as it is often broken into smaller chunks and saved on different servers beyond the reach of DFPs. Malware placed in the RAM requires expensive RAM Forensics. The depth of DFI can be restricted by legal challenges. Data is often acquired in a non-forensically sound manner DFPs. One of the methods to address this is to carry out triages a live system, which enables DFPs to extract evidence that can be hidden in volatile digital artefacts (such as the contents of RAM, running processes, or active network connections). This approach is also essential to prevent losing evidential data considering that a reboot could result in encryption of the file system or deletion of temporary data.

## **2.5. Reverse Engineering**

Reverse engineering is the process of disassembling and analysing the binary of a captured executable, a malware, network traffic or other execution traces. Through this process, the reverse engineer converts the binary instructions of the malicious programme to code mnemonics in order to be able to establish what the malicious programme does. One of the challenges associated with the reverse engineering process is that it requires a significant amount of time. Furthermore, current approaches cannot properly address emerging threats employing anti-forensics methods such as: code obfuscation, data destruction, data contraception, data hiding, and multistage loading architectures (Caviglione et al., 2017). Evolving standards of the reliability of digital evidence can also pose challenges, such as

messaging origins from IP addresses or online digital photograph authentication (Losavio & Keeling, 2014). Lack of skills and competency is also a major concern. For instance, individuals have been wrongly convicted of wrongdoings due to the insufficient analysis of digital forensics evidence. As a result, this damages the credibility and utility of DF as a discipline and jeopardize punishing the innocent. Absence of standards for DFPs and questions as to the ability and ethical behaviour within the DF produce their own challenges (Elmaghraby & Losavio, 2014; Losavio et al., 2018). These challenges relate to the use of data from digital devices.

### **3. PARADIGMS FOR FUTURE STUDIES**

As identified, there are significant challenges that exist in the digital forensic field. However, these challenges present opportunities for new research in digital forensics. In the following section, these challenges are used to motivate future paradigms of further research, suggesting and prioritising necessary key advancements.

#### **3.1. Cloud Forensics**

A solution to preserve and acquire cloud data in a forensically sound manner is to develop a library of DF methodologies for the various cloud platforms and deployment models (Martini & Choo, 2012; Montasari, 2016b; Montasari et al., 2019; Montasari, 2016d). There is also a need for technical knowledge and more research into investigation procedures and recovery methods on VMs (Lim et al., 2012). It is imperative for a new generation of forensic tools and techniques to be developed in order to address the limitations of traditional forensic tools when analysing virtual systems. One of these techniques could be Virtual Machine Introspection (VMI), that has created the foundation for a number of original approaches (Xenproject, 2019) within the domains of both cyber-security and digital forensics. In addition, cryptographic verifications can also be used for authenticating data integrity in cloud storage when implemented correctly. Furthermore, there is an urgent need for interdisciplinary efforts which can connect the requirements and concepts of evidence rising from the legal field to what can be feasibly recreated and inferred algorithmically or in an exploratory manner (Wolthusen, 2009). Existing methodologies for incident handling are focused on infrastructures and operational models that are being increasingly outdated by cloud computing. Therefore, new methods will need to be developed that can offer guidance for cloud customers and CSPs towards effective incident handling in the cloud (Grobauer & Schreck, 2010).

One approach to defend against Rootkit in Hypervisor attacks, that can stem from VM-Level susceptibilities, is to implement a robust firewall as well as deploying an effective system that can vigorously monitor Instruction Detection System (IDS) and Intrusion Prevention System (IPS). Another approach to defend against hypervisor-based attacks can be to make the hypervisor codebase more reactionary to attacks by embedding a unique self-protection ability in the hypervisor that can offer lifetime control flow integrity. Furthermore, it might be possible to eradicate the hypervisor attack surface by facilitating the guest VMs operating natively on the underlying hardware while managing the capability to operate various VMs at the same time. Such an approach could potentially consist of four elements: (1) pre-allocation of processor cores and memory resources, (2) use of virtualized I/O devices, (3) slight changes to the guest OS to carry out all system discovery throughout boot up, and (4) avoiding indirection by linking the guest virtual to the underlying hardware (Szefer et al., 2011).

Therefore, there will be no need for a hypervisor to assign resources dynamically, imitate I/O devices, support system detection after boot-up, or map interrupts. Defence mechanisms for hypervisors should concentrate on hypervisor accuracy. Detailed input authentication, appropriate tracking of context modifications, complete initialization of control structures, complete deletion of sensitive data on process termination, and complete awareness of the underlying hardware's capabilities could decrease the hypervisor's attack surface. The imitation of I/O and networking devices shows to be the main reason for failure.



Therefore, hypervisor vendors must implement a small set of secure back-end drivers as opposed to offering a large number of virtual devices with overlapping functionality which can be difficult to manage (Perez-Botero et al., 2013).

Another defence mechanism is to safeguard kernel from an untrusted management OS through a protected virtualization architecture that can offer a secure run-time environment, network interface, and secondary storage for a guest VM. Such a defence mechanism could potentially mitigate the trusted computing base of security-critical guest VMs, resulting in enhanced security in an untrusted management environment as well as providing more secure remote computing services (Jang-Jaccard & Nepal, 2014). A different countermeasure can be to implement hardware-assisted monitoring techniques that can accurately identify the presence of rootkits within seconds of their installation and detect malicious alterations to a host's kernel in order to safeguard software integrity. A hardware-assisted tampering identification system can also be implemented as a countermeasure to safeguard the integrity of hypervisors and operating systems. This approach can take advantage of aspects of the microprocessor, System Management Mode (a CPU mode in 86 architecture), to obtain and communicate the complete state of a secure machine to a remote server (scrutinise the hypervisor). This approach can also deploy the SMM to evade the hypervisor for integrity measurement purposes, thus, providing protection against malicious activities that try to attack a hypervisor.

Last, but not least, tools and procedures must be developed in order to identify forensic data physically with specific timestamps while at the same time considering the jurisdictional issues. Digital forensic readiness – or proactive measures which include both operational and infrastructural readiness – can significantly assist cloud forensic investigations. Examples include, but are not limited to, preserving regular snapshots of storage, continually tracking authentication and access control, and performing object-level auditing of all accesses. Recording users' activity trails in virtual machines is also a significant factor since a VM can function in the same way as an actual physical system does. Once the investigators find traces of a VM on the host, they must analyse the VM as well as the host system. However, the lack of knowledge of VM platforms, the investigation process is often not clear. Furthermore, it would be difficult to analyse a VM if it is damaged, for instance, due to the structural features.

### **3.2. IoT Forensics**

Considering the ever-evolving nature of IoT devices, unique practice methods and techniques are required to conduct a successful investigation. As the Cyber Security threat landscape continues to evolve and become complex, equally DFPs will continually need to extend their skill sets to address the variety and complexity of IoT devices to keep up with such an evolution. Thus, it is of paramount importance to conduct new studies to secure mission-critical IoT applications. New systems that use state-of-the-art security methods and techniques are needed to be developed. An example of this can be the development of IP-compatible secure communications networks that are appropriate for resource-constrained devices. Such systems would necessitate careful, interconnected, system-wide design, and skilled network engineers to implement and maintain them. Also, the majority of IoT technologies have built-in flash to run a simple form of OS (reduced version) or real-time application executables. Since these devices do not make use of conventional hard drives that can be removed or are not running full computer OSs, new methods need to be developed to extract data from these devices. To extract potential evidence from IoT devices, advanced data recovery might be needed to be developed. For instance, data stored in wearable devices are often inaccessible. Even if data could be extracted from such devices, it would be possibly encrypted or stored in a non-standard data format for which a viewer has not been created yet. In these situations, advanced data parsing and carving are needed to extract meaningful content from the data extracted from the device.

Moreover, to deal with the forensic challenges posed by IoT-connected devices, cloud cybersecurity will need to be reviewed since each IoT device produces data that is stored in the cloud. Cloud cybersecurity policies must be blended with IoT infrastructure so as to provide timely

responses for suspicious activities (Watson & Dehghantanha, 2016). They must be reviewed in relation to evidence identification, data integrity, preservation, and accessibility. CSPs will need to ensure the integrity of the digital evidence acquired from cloud computing components in order to facilitate an unbiased investigation process in establishing the root cause of the cyberattack in IoT. Therefore, as the IoT paradigm is further developed, it becomes necessary to develop adaptive processes, accredited tools and dynamic solutions tailored to the IoT model.

### 3.3. Big Data Forensics

To address the issue of the BFD, the research community need to develop new tools (or the adaptation of the existing ones), techniques, and algorithms (such as machine learning techniques) that could be utilised in the unique context of DF for triage and analysis of BFD (such as disk images and network traffic dumps). Currently, there are only few DF tools that make use of MLAs for the triage and analysis of forensic data. On the other hand, the existing machine learning tools and libraries used in 'data science' such as MapReduce are not fit or court-approved for use in the context of DF. Thus, such tools can be adapted to the task of processing the big data sets in DF with a parallel, distributed algorithm on a cluster. Similarly, Neural Networks can be extended to facilitate the complex pattern recognition in various branches of DF such as Cloud Forensics and Network Forensics. The research community should also focus their attentions on building upon Natural Language Processing (NLP) techniques, including Bayesian classifiers and unsupervised algorithms for authorship verification or classification of large bodies of unstructured texts.

The increasing use of artificial intelligence (AI) technologies in security applications, including forensics, has motivated the recent research paradigm of Explainable AI, including applications in cyber security. This research paradigm focusses on developing 'opaque' AI systems, ensuring that users of AI systems are able to fully understand what the AI system is doing (e.g., classification, decision making, etc.), which is becoming increasingly important in areas where AI are used in critical processes. For example, medical care. The same important applies to digital forensics, and there is a great need to ensure that AI technology is fully communicated to the user. This will ensure the user correctly understands the output and its relationship to the investigation, but most important, allows anyone involved in a legal process to understand, question, and gain an undisputed understanding of the outcome.

Furthermore, to address the main challenges of BFD (i.e. the 3Vs: volume, variety and velocity), in certain circumstances, it might become necessary to alter the conventional principles and procedures that 'all data' must be extracted in a 'strict' forensically-sound manner. Therefore, techniques related to the main phases of DF process (i.e. Identification, Acquisition, and Analysis) must be adapted to the context of big data. For instance, concerning the Acquisition Phase, proper triage procedures (determined by the type of investigation at hand and also case intelligence) must be carried out (often at the crime scene) when conventional 'bit-by-bit' copy is not possible due to the sheer volume of data. This denotes that investigators should scan 'all' data but only extract the parts applicable to the investigation. In these scenarios, investigators might need to access original source of evidence (Montasari & Hill, 2019; Montasari, 2016c). If this is the case, they must be able to justify and document their actions so as to adhere to the Principle two of the ACPO Guidelines, "In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions." (ACPO, 2012). One of the ways in which proper prioritisation or triage can be conducted is through visualization, both for low-level file system analysis and higher-level content analysis.

### 3.4. Encryption

One of the methods to address the encryption issues is to conduct RAM Forensic, which enables DFPs to acquire the current state of a digital device in a manner that would not be likely utilising disk examination on its own. This method requires imaging the RAM using a tool such as Belkasoft

Live RAM Capturer and then draw out a binary decryption key from that RAM image. However, the development of RAM Forensic tools is more challenging than the creation of disk tools. Data stored in disks is persistent and intended to be read back in the future. However, data written to RAM can only be read by the running program. The author in (Garfinkel, 2010) argues that as a result there is less desire “for programmers to document data structures from one version of a program to another”. Therefore, issues as such can complicate the task of tool developers. Furthermore, many of encryption schemes are implemented to resist brute-force attacks. There are currently several exploits that DFPs can leverage to overcome this implementation. For instance, DFPs can decrypt a BitLocker volume by determining the correct Microsoft Account password. This can be achieved by recovering the matching escrow key directly from Microsoft Account. There are various tools and methods, the discussion of which is outside the scope of this paper, for retrieving the password. Another method of exploit is to image the RAM using a tool such as Belkasoft Live RAM Capturer and then draw out a binary decryption key from that RAM image.

### **3.5. New Tools, Techniques and Standards**

By default, the existing DFI tools are designed to run on the perpetrator’s device. However, these tools provide restricted ability to examine complex cyberspace such as cloud sources. Therefore, many of the DFIs tools are inappropriate to discover anomalies in an automatic manner (Caviglione et al., 2017; Garfinkel, 2010). As a result, one of the key problems that need to be addressed as future research relates to the development of new tools and methods to examine the volume of data and provide potential digital clue to the DFPs for additional examination. However, the design and implementation of such tools and techniques are a complex task due to the absence of standardisation and computational requirements. Similarly, DFPs can take advantage of the element of cloud computing, for example, to reduce the most challenging processes of a DFI, such as log examination, data reduction, indexing and carving. Furthermore, analysing complex cyber-attacks necessitates a united and collaborative effort when processing information or when utilising outsourced storage and computation. For instance, the development of standard formats and abstractions require a collaborative approach to address the challenges of identification and extraction of digital artefacts from common and uncommon locations in various types of digital devices (Montasari & Peltola, 2015) and their subsequent categorisation and analysis. Furthermore, to enhance DF research, it is vital to implement standards for case data, data abstractions, and “composable models” for DF processing. There are five broadly utilised abstractions including: disk images, packet capture files, files, file signatures and Extracted Named Entities. Due to the absence of standardised data abstractions and data formats, researchers are often made to implement more parts of a system prior to being able to create initial results. As a result, this hinders their progress. Therefore, new abstractions are needed to be developed in order to represent and compute with large amount of data (Garfinkel, 2010).

### **3.6. Digital Forensics as a Service**

Digital Forensics as a Service (DFaaS) is an extension of the traditional DF process. DFaaS can be used to reduce the backlog of DF cases. DFaaS solution can address issues such as the storage, automation, investigators’ queries in the cases in which they are responsible. Furthermore, it facilitates efficient resource management, allows DFPs detectives to query data directly and enables easier teamwork amongst DFPs. Although DFaaS already provides multiple benefits, there are still many enhancements that can be made to the existing model in order to accelerate the existing process. For instance, such improvements can be made in relation to DFaaS’ functionality indexing capabilities and identification of incriminating evidence during the Collection Phase in a DFIP. However, it should be noted that DFaaS is not devoid of drawbacks, one of which pertains to latency concerning the online platform. Furthermore, DFaaS relies on the upload bandwidth available during the physical storage of data acquired through the Collection Phase in a DFIP (Lillis et al., 2016).

### 3.7. Distributed, HPC and Parallel Processing

Although the research community have investigated Distributed Digital Forensics (Roussev & Richard, 2004), there is more scope for research in this area. The processing speed of existing DF tools is insufficient for the average case. This is due to the fact that users have not been able to define clear performance requirements and that developers have not prioritised performance in accordance with reliability and accuracy. Therefore, new methods are needed to be developed to enable data collection in such a way that facilitates file-centric processing without disrupting optimal data throughput from the raw device (Montasari & Hill, 2019; Lillis et al., 2016). Furthermore, the benefits of High-Performance Computing (HPC) should be considered to decrease computation time and the time needed by the users. HPC methods, which leverage a degree of parallelism, have not been adequately investigated by researchers in the field of DF. HPC methods and hardware could be used for various purposes such as accelerating each phase in a Digital Forensic Investigation Process following the Collection Stage, i.e., Storage, Examination, Even Reconstruction, and Presentation and Reporting etc.

## 4. CONCLUSION

The field of DF is facing various challenges that are often difficult to overcome. As the new technologies are constantly being developed, LEAs are presented with numerous challenges that can have considerable socioeconomic impact on both global enterprises and individuals (Montasari & Hill, 2019; Caviglione et al., 2017; Jang-Jaccard & Nepal, 2014). Evidential data is no longer restricted to a single host but instead distributed between different or virtual locations. Furthermore, the rapid growth of Information and communication technologies (ICTs), as demonstrated in the Internet of Things (IoT), create substantial computable data that poses significant challenges and security risks. Furthermore, due to the heterogeneous nature of the IoT devices, the ways in which data is distributed, aggregated, and processed presents challenges to digital forensics investigations. Thus, in order to address the many challenges facing DF but also to take advantage of the opportunities it is presenting, the research community will need to reassess DF by, for instance, reconsidering the established principles and restructuring recognised workflows.

New methods of data reduction (for instance based on Machine Learning techniques) must be developed in order to reduce the large volumes of BDFD while at the same time preserving evidentiary data in native source file formats. For example, new techniques can be developed to facilitate the storage of data subsets in standard DF logical containers that can be processed and analysed by various DF tools. The new techniques should also be able to facilitate the mounting of data subsets as logical drives for processing and analysis again in various DF tools. The implementation of such methods can, subsequently, pave the way for collation and merging of varied data acquired from a wide variety of IoT devices for the purposes of processing and analysing BDFD in a timely manner. Furthermore, LEAs and the research community will need to adopt a more targeted approach to the IoT forensic investigations of digital evidence and a more efficient use of forensic laboratories. DF specialists need to undergo constant training and resource constraints should be mitigated by providing additional budgets to LEAs. The LEAs will also need to have their own bespoke, well-resourced DF units with teams of full-time DFPs, each of which should have up-to-date training and licences to use several different analytical tools. New techniques are required to overcome these challenges and leverage the architectures and processes employed in IoT in order to gain access to this rich source of potential evidence.

Last, but not least, worldwide collaboration among LEAs, academic institutions and corporates must be prioritised. Without a clear plan to facilitate research efforts that extend one another, forensic research will lag behind, tools will become outdated, and law enforcements' products will be incapable of relying on the results of DF analysis (Montasari & Hill, 2019; Garfinkel, 2010). Thus, the aforementioned entities will need to converge regularly to discuss the future of the discipline

and work out how to address the challenging aspects of the field. Likewise, more skills, tools and time are required to reconstruct digital evidence in a forensically sound manner. We believe that the future research directions outlined in this paper can have a positive impact on further research in the field of DF.

## REFERENCES

- ACPO. (2012). *ACPO Good Practice Guide for Digital Evidence*. Retrieved from [https://www.digital-detective.net/digital-forensics-documents/ACPO\\_Good\\_Practice\\_Guide\\_for\\_Digital\\_Evidence\\_v5.pdf](https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf)
- Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., & Peacock, M. et al. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, 22, 3–13. doi:10.1016/j.diin.2017.06.015
- BBC. (2017). *Cybercrime and fraud scale revealed in annual figures*. Retrieved from <https://www.bbc.co.uk/news/uk-38675683/>
- Beebe, N., & Clark, J. (2005). Dealing with terabyte data sets in digital investigations. In *Advances in Digital Forensics. DigitalForensics 2005. IFIP — The International Federation for Information Processing*, Boston, MA (pp. 3–16). Springer.
- Cameron, L. M. (2018). *Future of Digital Forensics Faces Six Security Challenges in Fighting Borderless Cybercrime and Dark Web Tools*. Retrieved from <https://publications.computer.org/security-and-privacy/2018/03/01/digital-forensics-security-challenges-cybercrime/>
- Casey, E., Ferraro, M., & Nguyen, L. (2009). Investigation delayed is justice denied: Proposals for expediting forensic examinations of digital evidence. *Journal of Forensic Sciences*, 54(6), 1353–1364. doi:10.1111/j.1556-4029.2009.01150.x PMID:19761473
- Casey, E., & Stellatos, G. J. (2008). The impact of full disk encryption on digital forensics. *Operating Systems Review*, 42(3), 93–98. doi:10.1145/1368506.1368519
- Catteddu, D. 2010. Cloud Computing: benefits, risks and recommendations for information security. *Proceedings of the Iberic Web Application Security Conference ENISA*, Greece. Springer (pp. 17-17). Academic Press. doi:10.1007/978-3-642-16120-9\_9
- Caviglione, L., Wendzel, S. & Mazurczyk, W., 2017. The future of digital forensics: Challenges and the road ahead. *IEEE Security & Privacy*, 15(6), 12-17.
- Chen, G., Du, Y., Qin, P., & Du, J. 2012. Suggestions to digital forensics in Cloud computing ERA. *Proceedings of the 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content*, Beijing, China (pp. 540-544). IEEE. doi:10.1109/ICNIDC.2012.6418812
- Farsi, M., Daneshkhah, A., Far, A. H., Chatrabgoun, O., & Montasari, R. (2019). Crime Data Mining, Threat Analysis and Prediction. In H. Jahankhani (Ed.), *Cyber Criminology* (pp. 183–202). Berlin, Germany: Springer.
- CSA. (2009). *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*. Retrieved from <https://cloudsecurityalliance.org/artifacts/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v1-0/>
- Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4), 491–497. doi:10.1016/j.jare.2014.02.006 PMID:25685517
- Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7, 64–73. doi:10.1016/j.diin.2010.05.009
- Grobauer, B., & Schreck, T. 2010. Towards incident handling in the cloud: challenges and approaches. *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, Chicago, IL (pp. 77-86). ACM. doi:10.1145/1866835.1866850
- Hosseinian-Far, A., Ramachandran, M., & Slack, C. (2017). Emerging Trends in Cloud Computing, Big Data, Fog Computing, IoT and Smart Living. In M. Dastbaz, H. Arabnia, & B. Akhgar (Eds.), *Technology for Smart Futures* (pp. 29–40). London: Springer.
- Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In B. Akhgar, A. Staniforth, & F. Bosco (Eds.), *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 149–164). London: Elsevier. doi:10.1016/B978-0-12-800743-3.00012-8
- Jahankhani, H., & Hosseinian-Far, A. (2015). Challenges of Cloud Forensics. In V. Chang, M. Ramachandran, R. J. Walters, & G. Wills (Eds.), *Enterprise Security* (pp. 1–18). Vancouver, Canada: Springer.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973–993. doi:10.1016/j.jcss.2014.02.005

Khan, S., Gani, A., Abdul Wahab, A. W., Iqbal, S., Abdelaziz, A., Mahdi, O. A., & Chang, V. et al. (2016). Towards an Applicability of Current Network Forensics for Cloud Networks: A SWOT Analysis. *IEEE Access : Practical Innovations, Open Solutions*, 4, 9800–9820. doi:10.1109/ACCESS.2016.2631543

Kuo, C.-T., Chi, P.-W., Chang, V., & Lei, C.-L. (2018). SFaaS: Keeping an eye on IoT fusion environment with security fusion as a service. *Future Generation Computer Systems*, 86, 1424–1436. doi:10.1016/j.future.2017.12.069

Lillis, D., Becker, B. A., O'Sullivan, T., & Scanlon, M. 2016. Current Challenges and Future Research Areas for Digital Forensic Investigation. *Proceedings of the 11th Annual ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*, Daytona Beach, FL. Academic Press.

Lim, S., Yoo, B., Park, J., Byun, K. D., & Lee, S. (2012). A research on the investigation method of digital forensics for a VMware Workstation's virtual machine. *Mathematical and Computer Modelling*, 55(1-2), 151–160. doi:10.1016/j.mcm.2011.02.011

Losavio, M. M., Chow, K. P., Koltay, A., & James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. *Security and Privacy*, 1(3), 23. doi:10.1002/spy.2.23

Losavio, M. M., & Keeling, D. (2014). Evidentiary power and propriety of digital identifiers and the impact on privacy rights in the United States. *Journal of Digital Forensics, Security and Law*, 9(2), 16.

Lukan, D. (2014). *Cloud Forensics: An Overview*. Retrieved from <https://resources.infosecinstitute.com/overview-cloud-forensics/>

Martini, B., & Choo, K.-K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, 9(2), 71–80. doi:10.1016/j.diin.2012.07.001

Mislan, R. P., Casey, E., & Kessler, G. C. (2010). The growing need for on-scene triage of mobile devices. *Digital Investigation*, 6(3-4), 112–124. doi:10.1016/j.diin.2010.03.001

Montasari, R. (2016a). A comprehensive digital forensic investigation process model. *International Journal of Electronic Security and Digital Forensics*, 8(4), 285–302. doi:10.1504/IJESDF.2016.079430

Montasari, R. (2016b). An ad hoc detailed review of digital forensic investigation process models. *International Journal of Electronic Security and Digital Forensics*, 8(3), 205–223. doi:10.1504/IJESDF.2016.077444

Montasari, R. (2016c). Formal two stage triage process model (FTSTPM) for digital forensic practice. *International Journal of Computer Science and Security*, 10, 69–87.

Montasari, R. (2016d). Review and assessment of the existing digital forensic investigation process models. *International Journal of Computers and Applications*, 147(7), 41–49. doi:10.5120/ijca2016911194

Montasari, R. (2016e). *The Comprehensive Digital Forensic Investigation Process Model (CDFIPM) for Digital Forensic Practice* [thesis]. University of Derby, Derby, UK.

Montasari, R. (2017a). A standardised data acquisition process model for digital forensic investigations. *International Journal of Information and Computer Security*, 9(3), 229–249. doi:10.1504/IJICS.2017.085139

Montasari, R. (2017b). An Overview of Cloud Forensics Strategy: Capabilities, Challenges, and Opportunities. In A. Hosseinian-Far, M. Ramachandran, & D. Sarwar (Eds.), *Strategic Engineering for Cloud Computing and Big Data Analytics* (pp. 185–205). London: Springer. doi:10.1007/978-3-319-52491-7\_11

Montasari, R. (2017c). Digital Evidence: Disclosure and Admissibility in the United Kingdom Jurisdiction. In H. Jahankhani et al. (Eds.), *Global Security, Safety and Sustainability - The Security Challenges of the Connected World* (pp. 42–52). London, UK: Springer.

Montasari, R. (2018). Testing the Comprehensive Digital Forensic Investigation Process Model (the CDFIPM). In M. Dastbaz, H. Arabnia, & B. Akhgar (Eds.), *Technology for Smart Futures* (pp. 303–327). Springer. doi:10.1007/978-3-319-60137-3\_15

- Montasari, R., Carpenter, V., & Hill, R. (2019). A road map for digital forensics research: A novel approach for establishing the design science research process in digital forensics. *International Journal of Electronic Security and Digital Forensics*, 11(2), 194–224. doi:10.1504/IJESDF.2019.098784
- Montasari, R., & Hill, R. (2019). Next-Generation Digital Forensics: Challenges and Future Paradigms. In H. Jahankhani & A. Hosseinian-Far (Eds.), *Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)* (pp. 205-212). London: IEEE.
- Montasari, R., Hill, R., Carpenter, V., & Hosseinian-Far, A. (2019). Evaluation of the Standardised Digital Forensic Investigation Process Model (ESDFIPM). In H. Jahankhani (Ed.), *Cyber Security Practitioner's Guide*. World Scientific.
- Montasari, R., Hill, R., Carpenter, V., & Hosseinian-Far, A. (2019). The Standardised Digital Forensic Investigation Process Model (SDFIPM). In H. Jahankhani et al. (Eds.), *Blockchain and Clinical Trial* (pp. 169–209). London: Springer. doi:10.1007/978-3-030-11289-9\_8
- Montasari, R., Hill, R., Carpenter, V., & Montasari, F. (2019). Digital Forensic Investigation of Social Media, Acquisition and Analysis of Digital Evidence. *International Journal of Strategic Engineering*, 2(1), 52–60. doi:10.4018/IJoSE.2019010105
- Montasari, R., & Peltola, P. (2015). Computer Forensic Analysis of Private Browsing Modes. In H. Jahankhani et al. (Eds.), *Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security. ICGS3 2015. Communications in Computer and Information Science* (pp. 96–109). London: Springer.
- Montasari, R., Peltola, P., & Evans, D. (2015). Integrated Computer Forensics Investigation Process Model (ICFIPM) for Computer Crime Investigations. In H. Jahankhani et al. (Eds.), *Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security. ICGS3 2015. Communications in Computer and Information Science* (pp. 83–95). London, UK: Springer.
- Palmer, G. 2001. A road map for digital forensic research. *Proceedings of the First Digital Forensic Research Workshop*, Utica, New York (pp. 27-30). Academic Press.
- Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Transactions on Intelligent Transportation Systems*, 18(11), 2898–2915. doi:10.1109/TITS.2017.2665968
- Perez-Botero, D., Szefer, J., & Lee, R. B. 2013. Characterizing hypervisor vulnerabilities in cloud computing servers. *Proceedings of the 2013 international workshop on Security in cloud computing*, Hangzhou, China (pp. 3-10). ACM. doi:10.1145/2484402.2484406
- Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation*, 13, 38–57. doi:10.1016/j.diin.2015.03.002
- Quick, D., & Choo, K.-K. R. (2014). Data reduction and data mining framework for digital forensic evidence: Storage, intelligence, review and archive. *Trends and Issues in Crime and Criminal Justice*, 480, 1–11.
- Quick, D., & Choo, K.-K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, 11(4), 273–294. doi:10.1016/j.diin.2014.09.002
- Roussey, V., & Richard, G. 2004. Breaking the Performance Wall - The Case for Distributed Digital Forensics. In: *Proceedings of the 2004 digital forensics research workshop*. Baltimore, MD: DFRWS, pp. 1-16.
- Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud Forensics. In G. Peterson & S. Sheno (Eds.), *Advances in Digital Forensics VII* (pp. 35–46). Berlin: Springer.
- Szefer, J., Keller, E., Lee, R. B., & Rexford, J. 2011. Eliminating the hypervisor attack surface for a more secure cloud. In: *Proceedings of the 18th ACM conference on Computer and communications security*. Chicago, Illinois, USA: ACM, pp. 401-412. doi:10.1145/2046707.2046754
- Watson, S. & Dehghantanha, A., 2016. Digital forensics: the missing piece of the Internet of Things promise. *Computer Fraud & Security*, 2016(6), pp. 5-8.
- Wolthusen, S. D. 2009. Overcast: Forensic Discovery in Cloud Environments. *Proceedings of the 2009 Fifth International Conference on IT Security Incident Management and IT Forensics*, Stuttgart, Germany (pp. 3-9). IEEE. doi:10.1109/IMF.2009.21



Xenproject. (2019). *Virtual Machine Introspection*. Retrieved from <https://tinyurl.com/yb4h3bc5/>

Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2019). Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. *Information Sciences*, 479, 567–592. doi:10.1016/j.ins.2018.02.005

*Reza Montasari (PhD) is a Senior Lecturer in Cyber Security in the Department of Computer Science at the University of Huddersfield. Dr. Montasari has held a number of academic teaching and research positions over the past 6 years and have published widely in the fields of digital forensics, cyber security, Cloud computing and Internet of Things (IoT) security. Dr. Montasari is a Fellow of the Higher Education Academy (FHEA), a Chartered Engineer (CEng) registered with the Engineering Council and a Member of The Institution of Engineering and Technology (MIET).*

*Simon Parkinson has an honours degree in secure and forensic computing and a PhD in the cross-discipline use of domain-independent artificial intelligence planning to autonomously produce measurement plans for machine tool calibration. This resulted in the ability to produce measurement plans to reduce both machine tool downtime and the uncertainty of measurement. His research interests are in developing intelligent systems for manufacturing and cyber security. This involves his continuing research of developing and utilising artificial intelligence for task automation. His research interests are cyber security focused and cover aspects such as access control, vulnerability and anomaly detection, learning domain knowledge, mitigation planning, and software tools to aid situation awareness*

*Dr Amin Hosseini-Far is a Senior Lecturer in Business Systems and Operations; He is also the Chair of the research Centre for Sustainable Business Practices (CSBP) at the University of Northampton. In his previous teaching experience, Amin was a Staff Tutor at the Open University, and prior to that a Senior Lecturer and Course Leader at Leeds Beckett University. He has held lecturing and research positions at the University of East London, and at a number of private HE institutions and strategy research firms. Dr Hosseini-Far has also worked as Deputy Director of Studies at a large private higher education institute in London. Dr Hosseini-Far received his BSc (Hons) in Business Information Systems from the University of East London, an MSc degree in Satellite Communications and Space Systems from the University of Sussex, a Postgraduate Certificate in Research and a PhD degree titled 'A Systemic Approach to an Enhanced Model for Sustainability' which he acquired from the University of East London. He has more than 50 peer-reviewed publications that are disseminated as journal articles, conference papers and book chapters. Moreover, he has been an editor of two books and two conference proceedings. Amin holds the Membership of the Institution of Engineering and Technology (IET), the Senior Fellowship of the Higher Education Academy (HEA), and the Fellowship of the Royal Society of Arts (RSA). He is also an Associate Editor for the International Journal of Systems and Society, and the founding editor and the Editor-in-Chief of the International Journal of Strategic Engineering (IJoSE).*