A Framework for Cloud Forensic Readiness in Organizations

Ahmed Alenezi, Raid Khalid Hussein, Robert J. Walters and Gary B. Wills
Electronics and Computer Science
University of Southampton
Southampton, UK
{aa4e15, rkh2n14, rjw5, gbw}@soton.ac.uk

Abstract—**Many have argued that cloud computing is one of the fastest growing and most transformative technologies in the history of computing. It has radically changed the way in which information technologies can manage, access, deliver and create services. It has also brought numerous benefits to end-users and organizations. However, this rapid growth in cloud computing adoption has also seen it become a new arena for cybercrime. This has, in turn, led to new technical, legal and organizational challenges. In addition to the large number of attacks which affect cloud computing and the decentralized nature of data processing in the cloud, many concerns have been raised. One of these concerns is how to conduct a proper digital investigation in cloud environments and be ready to collect data proactively before an incident occurs in order to save time, money and effort. This paper proposes the technical, legal and organizational factors that influence digital forensic readiness for Infrastructure as a Service consumers.**

Keywords—Digital Forensics; Cloud Computing; Cloud Forensics; Cloud Forensic Readiness;

I. Introduction

The recent revolution in cloud computing has not only seen it become a new paradigm in information technologies, but has led many to view it as one of the fastest growing and most transformative technologies in the history of computing [1]. It has also changed the way in which information technologies can manage, access, deliver and create services [2]. There is a strong belief that one of the main reasons why cloud computing is considered to be one of the fast-growing technologies is because adopting cloud computing can reduce IT costs and maximize operational efficiency [3,4].

However, this rapid growth in cloud computing adoption means that cloud environments have become a new arena for cybercrime [1]. This has, in turn, led to new technical, legal and organizational challenges. In addition to the large number of attacks which affect cloud computing and the decentralized nature of data processing in the cloud, many concerns have been raised regarding how to conduct a proper digital investigation in cloud environments [1]. Ordinarily, if an attack occurs, investigations must be carried out without having to depend on a third party. However, in cloud environments this process remains complicated, since cloud providers, which have full power over the environment, control the sources of evidence and consumers are still not yet capable of proactively collecting data before an incident occurs [5]. In light of this, being forensically ready for digital investigations would save time and money.

According to Market Research Media [6], by 2020 it is expected that the global cloud computing market will grow by 30% CAGR (global compound annual growth), reaching approximately $270 billion. This estimation indicates that the cloud computing industry is growing, as is the number of cloud users around the world. However, this growth will also lead to a rise in the number of cyber-attacks.

This paper attempts to understand and identify the factors that contribute to cloud forensics readiness and how these factors can help to achieve forensics readiness. This paper is organized as follows: in Section II, we review the background of digital forensics and cloud computing. In section III, we discuss a number of valuable studies that have attempted to investigate digital forensic readiness. In section IV, we propose our Cloud Forensic Readiness Framework. Finally, this paper is concluded in Section V.

II. BACK GROUND

This section assesses the research background of digital forensics and cloud computing. Cloud computing deployment models, service models, and their characteristics are discussed in this section. Moreover, the field of digital forensics is reviewed, following which there is an overview of cloud forensics and its challenges. Finally, forensics readiness is introduced and related work is comprehensively discussed.

A. Digital Forensics

It is believed that digital forensics, as an independent field, was developed after the late 90s when the number of computer crimes increased as a result of the Internet's surging popularity [7]. Palmer [8] was the first to define digital forensics. It can be said that digital forensics is the process of analyzing electronic information that is stored in one or more digital machines to determine and reconstruct the sequence of events that lead to a specific incident.

B. Cloud Computing

Whilst it is well-known that cloud computing, as a technology, is not new to the field of computing, the actual term cloud computing was only introduced to the public in 2007, when Google and IBM announced a collaboration on cloud technologies [9]. The European Commission, Expert

Group report [10] defined cloud computing as a flexible execution environment of resources that includes a number of stakeholders and provides measured services at various granularities for a specified level of service.

From the user, provider, designer and architect perspectives, we can define cloud computing as a type of both parallel and distributed system that enables different users to benefit from sharing various computing resources as a service. Indeed, based on specific agreements with cloud providers, consumers are able to adjust, upgrade or change their service requirements at a lower cost.

The National Institute of Standards and Technology's (NIST) [11] description of cloud computing has been widely accepted; indeed, NIST has clearly defined four types of cloud deployment models, three different service models, and a number of essential and common characteristics. Cloud computing deployment models are classified as: *Public cloud* which is commonly owned by profitable organizations that sell services on a pay as you go basis (e.g. Google AppEngine) [3]; *Private cloud*, which provides services just as the public cloud does and can be managed by a third party but used only by one organization for specific usage (e.g. Microsoft Private Cloud) [11]; *Hybrid cloud* is a mix of public and private clouds which gives consumers more flexibility than private and public clouds (e.g. VMware Hybrid Cloud) [12]; *Community cloud* shares the same infrastructures among a number of users in various organizations who share the same needs [13]. In contrast, cloud service models are classified as: *Software as a Service (SaaS)* which allows only cloud end-users to utilize cloud services over the Internet (e.g. GoogleApps) [11]; In *Platform as a Service (PaaS)* model, with which users can deploy and manage their own application in the cloud (e.g. Microsoft Azure) [14]; *Infrastructure as a Service (IaaS)*, whereby users can manage the applications, storages and the operating system but have less control over the network (e.g. Amazon Web Services AWS) [11].

C. Cloud Forensics

Cloud computing environments have become an attractive battleground for cybercrime in the last few years. Cloud forensics was defined by NIST [15] as "the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation and reporting of digital evidence". Whilst in conventional digital forensics it is possible for investigators to collect evidence and isolate targeted systems, in cloud environments many new challenges are faced, such as: unknown physical location, inaccessibility, multi-tenancy and multi-jurisdiction. In 2011, Ruan [1] was the first researcher to introduce the term Cloud Forensics. Indeed, she introduced technical, organizational and legal cloud forensics dimensional models, as well as their challenges. Furthermore, NIST [15] aggregated a list of 65 challenges for cloud forensics.

The numerous challenges that exist in cloud forensics have motivated many organizations to overcome these issues by being forensically ready to undertake digital investigation in cloud environments, which will be introduced in the following section.

D. Cloud ForensicsReadiness

The increased number of security breaches in cloud environments has shown many organizations how severe the need for Cloud Forensics Readiness is [16]. Indeed, a recent cloud forensics survey [17] revealed that more than 80% of the respondents who were familiar with digital forensics expressed the need for "a procedure and a set of toolkits to proactively collect forensic-relevant data in the cloud is important". In order for any system to be forensically ready, two main objectives must be satisfied: maximizing the ability to acquire digital evidence, and reducing the costs of any digital forensics investigations [18]. Consequently, cloud forensics readiness can be identified as a mechanism aimed at reducing the cost of carrying out an investigation in a cloud environment by providing any relevant information needed before setting up the investigation.

III. RELATED WORK

A number of valuable studies have attempted to investigate digital forensic readiness, and these will be discussed below:

Grobler et al. [19] identified certain goals and steps of proactive digital forensics, and six various dimensions of digital forensics. They proposed a theoretical digital forensics framework that can guide organizations in implementing proactive forensics. Moreover, Elyas et al. [20,21] developed a conceptual framework by identifying factors that can contribute to achieving forensic readiness in an organization.

Valjarevic and Venter [22] proposed implementation guidelines for a harmonized Digital Forensic Investigation Readiness Process (DFIRP) model that consists of three readiness processes (planning, implementation and assessment); this model was then added to ISO/IEC 27043, 2014. The proposed guidelines can help to implement digital forensic readiness measures in various organizations, thus resulting in effective and efficient digital forensics investigations that provide courts with admissible digital evidence.

Certain papers have highlighted the need for new tools and digital forensics techniques to investigate anti-forensics methods; these papers have also provided an automation of live investigations. Moreover, a systematic literature review was undertaken by Alharbi [23] in order to identify and map out the existing processes in the digital forensics literature. The review revealed only one process that supports proactive forensics. Consequently, a proactive and reactive digital forensics functional process was proposed.

Kebande and Venter [24] propose a model designed to achieve digital forensic readiness by implementing a Botnet as a service in a cloud environment. The main contribution of this model was that it transformed botnets from illegal to legal monitoring and information capturing applications that can be used to provide courts with admissible digital evidence. However, this model has yet be standardized so that it can support other proactive cloud processes.

Sibiya et al. [25] proposed a forensics readiness model that can be utilized by cloud providers as a technique for digital forensics readiness. This can help cloud providers to administer data which are needed for potential investigations. Nevertheless, the scope of this model is limited to examining the readiness of data for forensic analysis in a cloud environment.

Trenwith and Venter [26] propose a model designed to achieve digital forensics readiness in a cloud environment. The proposed model considers a remote and central logging facility which accelerates data collection. However, the model also addresses the collection of other forms of evidence which may be needed in digital forensic investigations.

Makutsoane and Leonard [27] proposed a conceptual framework for organizations that intend to migrate to cloud computing. The aim was to determine the state of readiness of Cloud Service Providers (CSPs). The proposed framework, which includes a process tool, enables organizations to make correct decisions and select the suitable CSPs.

Kebande and Venter [28] highlighted the needs of a cloud environment when using a non-Malicious Botnet to be ready for forensic investigations. These proposed requirements cover technical, operational and legal perspectives based on the ISO/IEC 27043:2015 standard. However, the requirements must also be tested for effectiveness and standardized in order to support future technologies.

A study by Moussa et al. [29] proposed a conceptual framework designed to help IaaS consumers be forensically ready. The framework illustrates how IaaS consumers can collect the required digital evidence without relying on cloud providers. The framework consists of nine components, including the technical, legal and organizational forensic readiness elements.

A forensic-by-design framework was proposed by Rahman et al. [30] for Cyber-Physical Cloud Systems (CPCS). Indeed, this framework highlighted the importance of forensic readiness. This conceptual framework, which comprises six factors, ensures that a CPCS is designed to ease forensic investigations. The forensic-by-design approach can support digital investigations by identifying and determining the source of evidence and by accelerating said investigations.

IV. THE PROPOSED FRAMEWORK

Although a number of studies have investigated digital forensics readiness, there remains little in the way of research concerning digital forensics readiness in cloud environments. As such, the aim of this research is to propose a framework to investigate the factors that influence the readiness of organizations to undertake cloud forensics. The proposed framework in this research is designed to aid the investigation of the technical, legal and organizational factors that influence the forensics readiness of cloud computing consumers.

A. Framework Development

The framework development process, as shown in Figure 1, is divided into two stages. During stage one, technical, legal and organizational factors were identified from both the academic literature review and industry standards, as illustrated in Table 1. Following this, during stage two, the identified factors have been evaluated and analyzed, with any duplications removed.

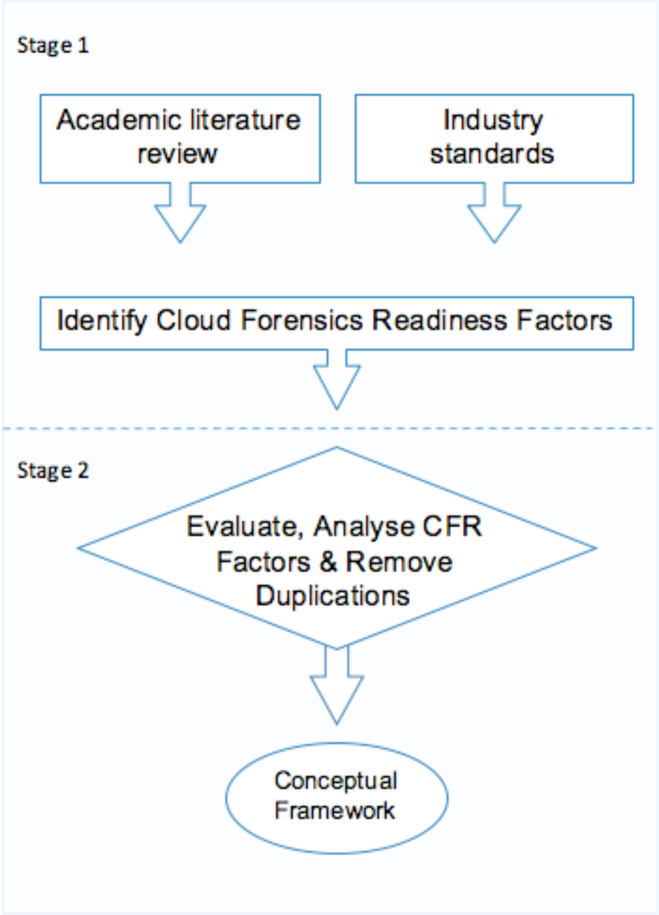
Stage 1
Academic literature review
Industry standards
Identify Cloud Forensics Readiness Factors
Stage 2
Evaluate, Analyse CFR Factors & Remove Duplications
Conceptual Framework

Figure 1: the framework development process.

B. The proposed Cloud Forensic Readiness Framework

The proposed Cloud Forensic Readiness framework, as illustrated in Figure 2, includes three categories: technical, legal and organizational factors. These factors are discussed below:

1) Technical Factors

The technical factors describe the technological aspects that influence forensic readiness in cloud environments.

- *Cloud infrastructure:* preparing the underlying infrastructure to support digital forensics investigations. Infrastructure preparation includes networking, system and laboratory.
- *Cloud architecture:* the system architecture must be designed in a specific way so as to increase its forensics capabilities, which results in the obtaining of admissible digital evidence.

- *Forensic technologies:* these include specialized forensic software or tools which are vital when it comes to collecting evidence in any digital investigation. It can be difficult to conduct a digital investigation without proper technology, and as a result these technologies should be reliable and accurate in order to provide admissible evidence.

- *Cloud security:* security programs are utilized in the digital forensics field as a trigger alarm. Thus, in order to conduct a digital investigation, incidents must first be detected by a monitor system in a timely manner. This can be achieved by using various technologies such as Intrusion Detection Systems (IDS), as well as Anti-virus and Anti-Spyware technology.

2) *Legal Factors*

legal factors include the aspects that are related to agreements between consumers and providers, multi-jurisdictions and regulatory authorities.

- *Service Level Agreement (SLA):* a contract between a cloud service provider (CSPs) and customers that documents what services the provider will offer, including forensics investigations. The SLA should clearly specify CSP and customers' responsibilities associated with forensic investigations.

- *Regulatory:* adherence to laws and regulations, such as admissibility of digital evidence in court and the chain of custody.

- *Jurisdiction:* judicial region. Since CSPs may provide cloud services from another region or area, it is necessary for organizations to determine the judicial regions, if any, and consider all multi-jurisdictions.

3) *Organizational Factors*

The organizational factors illustrate the characteristics of an organization and its employees that can facilitate cloud forensic readiness.

- *Management support:* refers to the top management level of an organization's support structure – the structure which helps the organization to become forensically ready. This includes authorization, decision making, funding, etc.

- *Readiness strategy:* an organization's plan to achieve forensics readiness. Generally speaking, the strategy pertains to how the readiness would work. This includes identifying hypothetical scenarios, possible evidence sources, and budget planning.

- *Governance:* concerns about the implementation of cloud forensics readiness in an organization. This includes managing procedures and responsibilities in order to collect evidence and attain a successful forensic investigation.

- *Culture:* the pattern of beliefs, values, assumptions and practices that have a direct impact on the implementation of digital forensics. Understanding culture before implementing digital forensics is very important, as it leads to successful potential forensics investigations.

- *Training:* the provision of training programs to technical staff and awareness programs to non-technical staff on forensics best practices.

- *Procedures:* a number of guidelines, procedures and instructions designed to guide the digital forensics investigations. These include proactive and reactive forensic procedures.

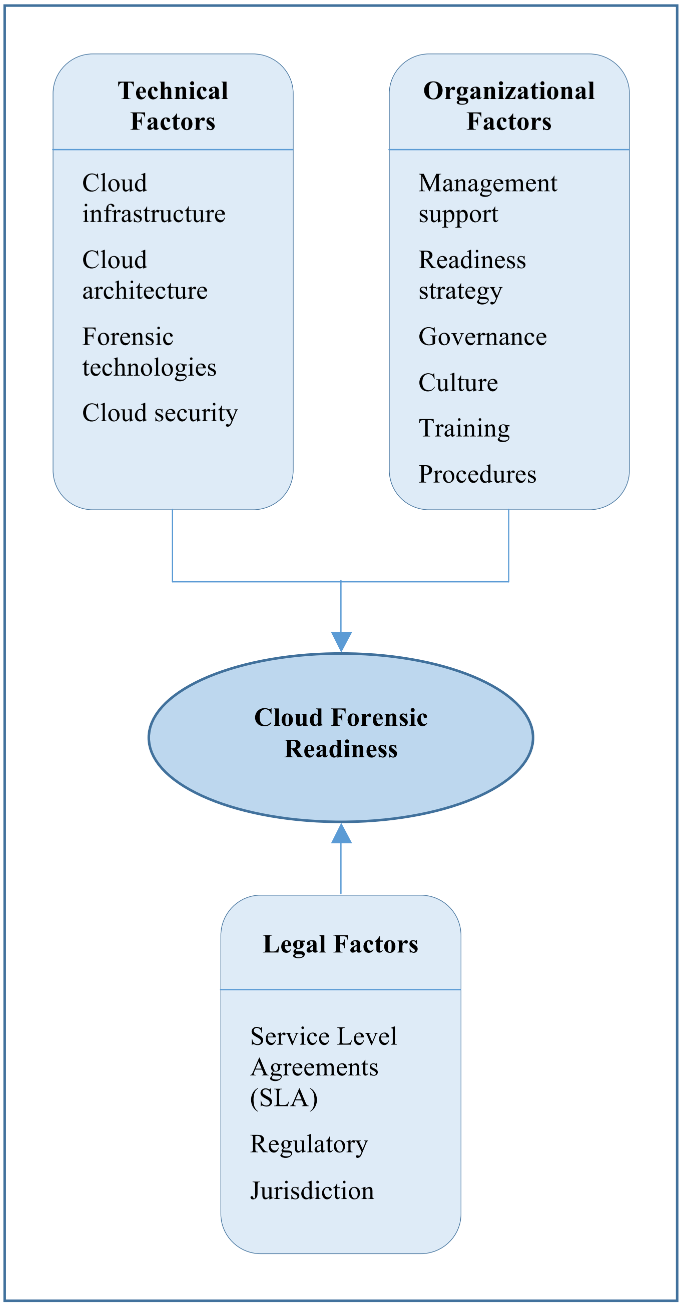

Figure 2: Cloud Forensic Readiness Framework.

Table 1: Forensic readiness factors mapped to the literature.

Study	Forensics Readiness Factors												
	Technical Factors				Legal Factors			Organizational Factors					
	Infrastructure	Architecture	Technologies	Security	SLA	Regulatory	Jurisdiction	Management support	Strategy	Governance	Culture	Training	procedure
Grobler et al. [19]	√		√			√	√			√	√	√	√
Elyas et al [20]		√	√			√		√		√	√	√	
Elyas et al. [21]	√	√	√			√		√		√	√	√	
Sibiya et al. [25]	√		√	√									
Makutsoane & Leonard [27]			√		√		√		√				√
Kebande & Venter [28]		√	√	√			√						
Moussa et al. [29]			√	√			√		√	√		√	√
Ab Rahman et al. [30]	√		√	√		√	√		√				
ACPO [31]												√	√
CSA [32]		√		√	√	√	√						√
ENISA [33]			√		√		√						√
ISO [34]		√		√			√						√

V. Conclusion and future work

The increased usage of cloud services brings with it a growth in the number of potential cyber threats. This has given rise to many new technical, legal and organizational challenges for digital investigations. As such, cloud forensics should certainly not be considered an afterthought. Although cloud environments have become an attractive battleground for cybercrime, there is little in the way of research concerning forensics readiness in cloud environments. This paper has proposed a framework through which to identify the key technical, legal and organizational factors that influence the forensic readiness of organizations using cloud services. With regard to future work, the framework will be validated and confirmed by cloud forensics experts and a survey will be distributed to a number of practitioners.

References

[1] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud Forensics: An Overview," *IFIP Conference on Digital Forensics*, pp. 35–46, 2011.

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599–616, 2009.

[3] A. Alharthi, M. O. Alassafi, R. J. Walters, and G. B. Wills, "An exploratory study for investigating the critical success factors for cloud migration in the Saudi Arabian higher education context," Telematics and Informatics, vol. 34, no. 2, pp. 664–678, 2016.

[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[5] L. Marco, M.-T. Kechadi, and F. Ferrucci, "Cloud Forensic Readiness: Foundations," *International Conference on Digital Forensics and Cyber Crime*, pp. 237–244, 2013.

[6] "MARKET RESEARCH MEDIA," *MARKET RESEARCH MEDIA*, 2016. [Online]. Available: http://www.marketresearchmedia.com/?p=839. [Accessed: 16-Jul-2016].

[7] S. Raghavan, "Digital forensic research: current state of the art," *CSI Transactions on ICT*, vol. 1, no. 1, pp. 91–114, 2013.

[8] G. Palmer, "A Road Map for Digital Forensic Research," *First Digital Forensic Research Workshop*, pp. 1–42, 2001.

[9] M. A. Vouk, "Cloud computing–Issues, research and implementations," *Journal of Computing and Information Technology*, vol. 16, no. 4, pp. 31–40, 2008.

[10] L. Schubert, K. Jeffery, and B. Neidecker-Lutz, "The future of cloud computing, opportunities for European Cloud computing beyond 2010.," *European Commission Information and Society Media - Expert Group Report*, 2010.

[11] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," 2011.

[12] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the-art and research challenges," *Journal of Internet Services and Applications*, vol. 1, no. 1, pp. 7–18, 2010.

[13] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "NIST Cloud Computing Reference Architecture," *NIST Special Publication 500-292*, vol. 292, no. 9, p. 35, 2011.

[14] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," *Proceedings of the Grid Computing Environments Workshop*, pp. 1–10, 2008.

[15] NIST Cloud Computing Forensic Science Working Group. (Draft NISTIR 8006), "NIST Cloud Computing Forensic Science Challenges," 2014.

[16] M. Hewling, "DIGITAL FORENSICS: AN INTEGRATED APPROACH FOR THE INVESTIGATION OF CYBER/COMPUTER RELATED CRIMES," 2013.

[17] K. Ruan, I. Baggili, J. Carthy, and T. Kechadi, "Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability : A Preliminary Analysis," *ADFSL Conference on Digital Forensics, Security and Law*, pp. 55–70, 2011.

[18] J. Tan, "Forensic Readiness," 2001.

[19] C. P. Grobler, C. P. Louwrens, and S. H. Von Solms, "A framework to guide the implementation of proactive digital forensics in organizations," *Availability, Reliability, and Security, 2010. ARES '10 International Conference*, pp. 677–682, 2010.

[20] M. Elyas, S. B. Maynard, A. Ahmad, and A. Lonie, "Towards a Systematic Framework for Digital Forensic Readiness," *Journal of Computer Information Systems*, vol. 54, no. 3, pp. 97–105, 2014.

[21] M. Elyas, A. Ahmad, S. B. Maynard, and A. Lonie, "Digital forensic readiness: Expert perspectives on a theoretical framework," *Computers and Security*, vol. 52, pp. 70–89, 2015.

[22] A. Valjarevic and H. Venter, "Implementation guidelines for a harmonised digital forensic investigation readiness process model," *2013 Information Security for South Africa*, pp. 1–9, 2013.

[23] S. Alharbi, J. Weber-Jahnke, and I. Traore, "The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review," *International Journal of Security and Its Applications*, vol. 5, no. 4, pp. 59–72, 2011.

[24] V. R. Kebande and H. S. Venter, "A Cloud Forensic Readiness Model Using a Botnet as a Service," *The International Conference on Digital Security and Forensics (DigitalSec2014)*, pp. 23–32, 2014.

[25] G. Sibiya, T. Fogwill, H. S. Venter, and S. Ngobeni, "Digital Forensic Readiness in a Cloud Environment," *AFRICON, IEEE*, pp. 1–5, 2013.

[26] P. M. Trenwith and H. S. Venter, "Digital forensic readiness in the cloud," *2013 Information Security for South Africa. IEEE*, 2013.

[27] M. P. Makutsoane and A. Leonard, "A conceptual framework to determine the digital forensic readiness of a Cloud Service Provider," *Proceedings of PICMET '14 Conference: Portland International Center for Management of Engineering and Technology; Infrastructure and Service Integration*, pp. 3313–3321, 2014.

[28] V. R. Kebande and H. S. Venter, "Requirements for Achieving Digital Forensic Readiness in the Cloud Environment Using an NMB Solution," *11th International Conference on Cyber Warfare and Security ICCWS*, 2016.

[29] A. N. Moussa, N. B. Ithnin, and O. A. . Miaikil, "Conceptual forensic readiness framework for infrastructure as a service consumers," in *Systems, Process and Control (ICSPC), 2014 IEEE Conference*, 2014, pp. 162–167.

[30] N. H. Ab Rahman, W. B. Glisson, Y. Yang, and K.-K. R. Choo, "Forensic-by-Design Framework for Cyber-Physical Cloud Systems," *IEEE Cloud Computing*, vol. 3, no. 1, pp. 50–59, 2016.

[31] J. Williams, "ACPO Good practice Guide for Digital Evidence.," *Metropolitan Police Service, Association of chief police officers, GB*, 2012.

[32] D. Birk and M. Panico, "Mapping the Forensic Standard ISO / IEC 27037 to Cloud Computing," *Cloud Security Alliance*, no. June, pp. 1–31, 2013.

[33] D. Liveri and C. Skouloudi, "Exploring Cloud Incidents," *The European Network and Information Security Agency (ENISA)*, no. June, pp. 1–14, 2016.

[34] ISO/IEC 27043. 2015. "Information technology — Security techniques — Incident investigation principles and processes".