Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH Open Access

Experts reviews of a cloud forensic readiness framework for organizations

Ahmed Alenezi[1,2*], Hany F. Atlam[2] and Gary B. Wills[2]

Abstract

Cloud computing has drastically altered the ways in which it is possible to deliver information technologies (ITs) to consumers as a service. In addition, the concept has given rise to multiple benefits for consumers and organizations. However, such a fast surge in the adoption of cloud computing has led to the emergence of the cloud as a new cybercrime environment, thus giving rise to fresh legal, technical and organizational challenges. In addition to the vast number of attacks that have had an impact on cloud computing and the fact that cloud-based data processing is carried out in a decentralized manner, many other concerns have been noted. Among these concerns are how to conduct a thorough digital investigation in cloud environments and how to be prepared to gather data ahead of time before the occurrence of an incident; indeed, this kind of preparation would reduce the amount of money, time and effort that is expended. As a number of cloud forensics challenges have not received enough attention, this study is motivated by a particular gap in research on the technical, legal and organizational factors that facilitate forensic readiness in organizations that utilize an Infrastructure as a Service (IaaS) model. This paper presents a framework with which to investigate the factors that facilitate the forensic readiness of organizations. This framework was identified by critically reviewing previous studies in the literature and by performing an in-depth examination of the relevant industrial standards. The factors were comprehensively studied and extracted from the literature; then, the factors were analysed, duplicates were removed, and the factors were categorized and synthesized to produce the framework. To obtain reliable results, the research method involved two steps: a literature review, followed by expert reviews. These techniques help us paint a comprehensive picture of the research topic and validate and confirm the results.

Keywords: Digital forensics, Cloud computing, Cloud forensics, Cloud forensic readiness

Introduction

The recent era has witnessed a cloud computing revolution; this revolution not only has led many to view the concept as a new IT paradigm but also has given cloud computing a reputation as one of the most rapidly growing and industry-changing technologies since the conception of computing itself [1]. In addition, this enormous surge has altered the way in which ITs can be used to access, manage, create and deliver services [2]. Many firmly believe that money is among the primary reasons cloud computing is thought of as a rapidly growing technology; indeed, adopting cloud computing in organizations can reduce the cost of IT [3].

However, the aforementioned lightning-fast growth in cloud computing adoption has led to a situation in which cloud environments are now viewed as a new environment for cybercrime. This situation has also given rise to fresh legal, organizational and technical challenges. At this point, it is appropriate to mention the substantial number of attacks that have an influence on cloud computing and the fact that cloud-based data processing is carried out in a decentralized manner; indeed, in addition to these factors, many have expressed concerns related to how a thorough digital investigation can be conducted in cloud environments [1]. In general, should any attack take place, it is essential to conduct investigations without the need to rely on a third party. However, the situation is different in cloud environments, where such a process is still complicated; these complications arise from the fact that cloud providers,

* Correspondence: aa4e15@soton.ac.uk
[1]Faculty of Computing and Information Technology, Northern Border University, Rafha, Saudi Arabia
[2]School of Electronics and Computer Science, University of Southampton, Southampton, UK

which fully dictate what happens in the environment, remain in control of the sources of evidence. In addition, consumers, to some extent, are still unable to proactively gather data prior to the occurrence of an incident [4]. Therefore, ensuring that forensic readiness is achieved before digital investigations are conducted would reduce the expenditure of both money and time.

According to Market Research Media [5], the worldwide cloud computing market is forecast to grow by a compound annual growth rate (CAGR) of 30% through 2020; at this point, many feel that the market will be worth approximately $270 billion. Such an estimation clearly illustrates the growth of the cloud computing industry, as well as the surge in the number of cloud users across the globe. Nevertheless, this growth will also give rise to an increase in the frequency with which cyberattacks are carried out. Although cloud forensics faces numerous challenges, there are no specially designed guidelines, procedures or standards pertaining to cloud forensics [6]. The investigation of this paper seeks to understand and identify the factors that contribute to cloud forensic readiness in organizations that utilize an Infrastructure as a Service (IaaS) model.

Motivation

As cloud environments have brought new challenges to the digital forensics field, the National Institute of Standards and Technology (NIST) [7] has identified 65 cloud forensics challenges. Aside from the vast number of attacks that have had an impact on cloud computing and the fact that cloud-based data processing is carried out in a decentralized manner, many other concerns have also been noted. Among these concerns are the issues of how to conduct a thorough digital investigation in cloud environments and how to prepare to gather data ahead of time prior to the occurrence of an incident; indeed, this kind of preparation would save money, effort and time. To the best of our knowledge, there are no standards or guidelines that focus on cloud environments at the time of writing/conducting this research. Consequently, we are motivated to investigate the influencing factors of cloud forensic readiness. The first essential is to understand the existing gaps and challenges faced by cloud consumers as they attempt to be forensically ready. Bearing this in mind, we propose the following research objectives:

- To fill the gaps in existing research regarding cloud forensic readiness.
- To identify the factors that contribute to forensic readiness in organizations that utilize an IaaS model.
- To verify the cloud forensic readiness framework.

To achieve the objectives of this study and contribute to the cloud forensics field, the following research question must be answered.

RQ1: What is the appropriate framework for cloud forensic readiness in organizations that utilize an IaaS model? This question is divided into three sub-questions:

Q1.1: What are the technological factors that influence cloud forensic readiness in organizations?
Q1.2: What are the legal factors that influence cloud forensic readiness in organizations?
Q1.3: What are the organizational factors that influence cloud forensic readiness in organizations?

The paper is structured as follows: The second section provides a literature review that discusses the concept of digital forensics and cloud forensics as well as some related. The third section proposes the cloud forensic readiness framework of this study; this proposal involves identifying all factors and mapping them to the literature. The fourth section outlines the research approach implemented during this study. The fifth section presents the study results, and the sixth section discusses the findings from the expert reviews. The final section provides an overview of the research and presents conclusions drawn from the results and future research directions.

Literature review

Since the technological revolution began in earnest in the late twentieth century, the number of crimes involving computers has grown dramatically. As a result, since that time, digital forensics has been employed to combat any attack or cybercrime and to improve and acquire legal evidence found in digital media. Digital forensics can be identified as the application of science to identify, acquire, examine and analyse data while maintaining data integrity and the chain of custody of the information [8, 9].

Many hold the belief that digital forensics, as a separate specialty, was pioneered during the late 1990s, just as the frequency of computer crimes began to rise due to the surge in the popularity of the Internet [10]. The recent era has seen an increase in the frequency of cyberattacks in cloud environments, and this increase is clear evidence of the ability that cybercriminals possess in regard to creating substantial and costly damage for both cloud providers and cloud customers [4]. The growing number of cybercriminals in cloud environments has resulted in more security breaches, which has prompted many organizations to embrace the need for cloud forensic readiness [11]. Moreover, the results of a cloud forensics survey by Ruan et al. [1] revealed that more than 80% of respondents who were familiar with digital forensics expressed that "*a procedure and a set of toolkits to proactively collect forensic-relevant data in the cloud is important*". Consequently, it is essential that cloud consumers achieve forensic readiness prior to the occurrence of any incident.

Service models are provided in cloud computing at three different levels: Software as a Service (SaaS), Platform as a Service (PaaS) and IaaS. Consumers have less control over an SaaS model, and the control level increases as we progress towards the IaaS model, as shown in Fig. 1. For instance, collecting evidence logs in a SaaS model exclusively depends on the cloud service provider (CSP). In contrast, in an IaaS model, the virtual machine image can be collected from the customer side [13]. As the aim of this research is to enable organizations to be forensically ready, our research scope focuses on the IaaS model, which provides consumers with a higher level of control.

This paper focuses on cloud forensic readiness from consumer perspectives, and for the purpose of this research, we can identify cloud forensic readiness as a mechanism that aims to reduce the cost of conducting an investigation in a cloud environment and to provide any relevant information needed before setting up an investigation. There is clear evidence showing that cloud forensic readiness can give rise to many benefits for cloud environments, including an enhanced security level. Marco et al. [4], Pangalos and Katos [14], and Alenezi et al. [15] agree that forensic readiness helps organizations improve their security strategies, be prepared for any attack, and reduce the number of security incidents.

Review of related work

In this paper, we critically reviewed previous studies in the literature and performed an in-depth examination of the relevant industrial standards. To paint a comprehensive picture of the research topic, five database sources that are considered the most relevant to the fields of computer science were selected: SpringerLink, the Association for Computing Machinery (ACM) Digital Library, the Institute of Electrical and Electronics Engineers (IEEE), ScienceDirect and Google Scholar. All of the searches were limited in date from 2010 to 2019. The queries used in this paper were as follows: (Cloud OR Digital) AND (Forensic OR Crime) AND (Readiness OR Framework OR Model OR Process OR Examination OR Analysis).

Numerous important studies have made attempts to explore digital forensic readiness, and the main studies are highlighted below:

Grobler et al. [16] identified certain goals and aims that accompany proactive digital forensics, as well as six diverse dimensions of digital forensics. They presented a theory-based digital forensics framework that is capable of guiding organizations as they begin to employ proactive forensics. Alharbi et al. [17], identified and mapped the processes that currently exist in the digital forensics literature. Doing so resulted in the proposal of a proactive and reactive digital forensics process. Moreover, Elyas [18, 19] formulated a conceptual framework by pinpointing factors that can contribute to the process of reaching a state of digital forensic readiness within organizations. Furthermore, Valjarevic and Venter [20] proposed guidelines related to the implementation of the harmonized digital forensic investigation readiness process (DFIRP) model. This model consists of three readiness processes: assessment, implementation, and planning; the model was then added to ISO/IEC 27043: 2015. The guidelines that were presented can assist in the

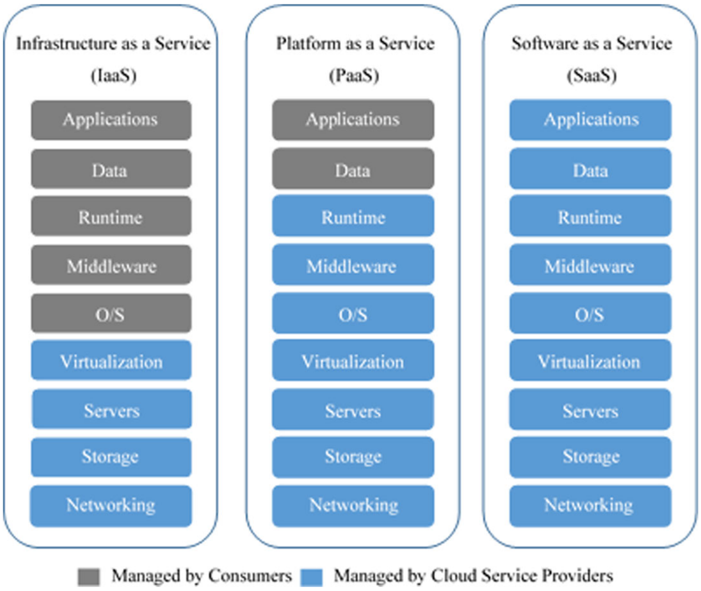

Fig. 1 Consumers' control over various models [12]

implementation of digital forensic readiness measures in a diverse range of organizations.

Moussa et al. [21] proposed a conceptual framework that aims to assist IaaS consumers in achieving forensic readiness. IaaS consumers can utilize the framework to establish how they should gather the necessary digital evidence without having to rely on cloud providers. However, the framework itself has yet to be verified or investigated empirically. A decision-making approach based on an algorithm was introduced by Simou, Troumpis and Kalloniatis [22] to calculate organizations' forensic readiness and compliance level and to categorize the unimplemented tasks in the cloud. Their aim was to identify important unimplemented tasks, classify them and prioritize them accordingly to provide useful information for both software engineers and stakeholders to make the appropriate decision. Similarly, Park et al. [23] introduced a digital forensic readiness model in cloud computing-based smart work. This model consists of two categories, namely, policy readiness and technical readiness. The authors conducted a validity analysis by distributing a survey to a number of digital forensic experts. However, not all evaluation criteria achieved scores that confirmed validity, and future research is expected to conduct an in-depth analysis of the proposed model for greater validity.

Sibiya et al. [24] introduced a forensic readiness model that can be employed by cloud providers as a technique to facilitate digital forensic readiness. This model can aid cloud providers in administering data that are necessary for any pending investigations. Regardless, the scope of the model means that it is limited to assessing data in terms of their readiness for cloud environment-based forensic analysis. Along similar lines, Makutsoane and Leonard [25] proposed a conceptual framework that can be used by organizations that have a tendency to switch to cloud computing. The aim behind their proposed framework was to determine the state of readiness of CSPs and to allow companies to make correct decisions regarding the most suitable CSPs.

A model aimed at facilitating digital forensic readiness through the implementation of a botnet service in a cloud environment was proposed by Kebande and Venter [26]. The primary contribution made by this model was the fact that it altered botnets, thus allowing them to transition from illegal to legal applications capable of monitoring and information capturing. The authors drew attention to the requirements that a cloud environment must meet when a non-malicious botnet is being used to prepare for forensic investigations [27]. All of the requirements proposed by these authors pertain to the legal, operational and technical aspects that emerge from the ISO/IEC 27043:2015 standard. Moreover, Kebande and Venter [28] examined the design and implementation of a cloud forensic readiness system. To function as an agent-based solution (ABS) in the cloud, a non-malicious botnet was employed by the authors. This technique is also aligned with ISO/IEC 27043: 2015, which enables organizations to conduct digital investigations without disrupting cloud operations.

In addition, a forensic-by-design framework was proposed by Ab Rahman et al. [29] for cyber-physical cloud systems (CPCSs). The framework clearly demonstrated exactly how important forensic readiness is. Such a conceptual framework, which is composed of six factors, guarantees that the design of a CPCS is based on the goal of simplifying and increasing the efficiency of forensic investigations. The forensic-by-design approach is supposed to be capable of facilitating digital investigations. In order for a judge to decide whether the presented evidence is trustworthy, Dykstra et al. [30] emphasized the importance of trust in cloud services. Their study investigated trust challenges during the collection of digital evidence in an IaaS model. Their proposed model is divided into six layers, and in each layer, various types of forensics activities and trust are required. However, their experiments were specific to an IaaS model using Elastic Compute Cloud (EC2) services. The study did not extent to other cloud service models because EC2 is the only model in which forensic tools can be installed.

Also of note here is a model that was presented by Trenwith and Venter [31] that aims to help reach a state of digital forensic readiness within a cloud environment. This model proposed the concept of using a remote and central logging facility that accelerates data gathering. Similarly, Zawoad et al. introduced Secure Logging as a Service (SecLaaS), which allows investigators to acquire the logs of virtual machines and to ensure the confidentiality of cloud users [32]. SecLaaS is supposed to protect the integrity of logs from any manipulation by providing proofs of past logs.

While numerous studies have investigated digital forensic readiness, a few studies have investigated digital forensic readiness in cloud environments. Moreover, to the best of our knowledge, this study is the first to have collected all of these factors together and to have analysed the way in which they affect cloud forensic readiness. Therefore, the goal of the present research is to propose and verify a framework that can facilitate organizations that utilize an IaaS model in achieving forensic readiness.

Proposed framework

As discussed above, the cloud environment is considered an issue in the field of digital forensics; for this reason, numerous challenges have emerged. The NIST

[7] has identified 65 cloud forensics challenges. As a result, cloud computing is viewed by many experts as a new cybercrime environment. Among these concerns are the issues of how to conduct a thorough digital investigation in cloud environments and how to prepare to gather data ahead of time prior to the occurrence of an incident; this preparation would save money, effort and time. To the best of our knowledge, a few studies have investigated cloud forensic readiness in general. To date, however, no other studies have gathered all of the influencing factors and introduced a verified framework that helps organizations that utilize an IaaS model be forensically ready. The following framework is proposed based on the literature review; the proposed framework was further elaborated in a previous research paper [15]. The framework consists of three dimensions, as depicted in Fig. 2: The proposed cloud forensic readiness framework [15].:

Technological factors

The technological factors describe the technological aspects that influence cloud forensic readiness in organizations. The following technological factors are related to digital forensic readiness and were identified by the literature review.

- **Cloud infrastructure**: Preparing the underlying infrastructure makes it possible to support and facilitate digital forensic investigations. Preparing the infrastructure helps organizations appropriately determine, trace and preserve potential evidence. Infrastructure preparation pertains to servers, storage, networks, operating systems, and digital forensic laboratories.
- **Cloud architecture**: The cloud architecture must be designed to increase its forensic capabilities. The correct architecture that supports cloud forensics will facilitate forensic procedures and make it possible to obtain admissible digital evidence.
- **Forensic technologies**: These technologies include specialized forensic software or hardware that can allow organizations to conduct a complete indoor digital investigation. They are considered vital when collecting and examining digital evidence in cloud environments. It can be difficult to conduct a digital investigation without proper technology, and therefore, these technologies should be reliable and accurate to produce admissible evidence.
- **Cloud security**: Security in cloud computing can be utilized in the digital forensics field as a trigger alarm to generate alert notifications when specified criteria are met and to provide a secure environment to facilitate the process of finding digital evidence and sources of evidence. Thus, to conduct a digital investigation, incidents must first be detected by a monitor system in a timely manner. Doing so can be achieved using various technologies, such as intrusion detection systems (IDSs), as well as anti-virus and anti-spyware technology. Moreover, the collected evidence must be securely gathered, transported and stored in a secure location.

Legal factors

The legal factors include aspects that are related to agreements between consumers and providers, multi-

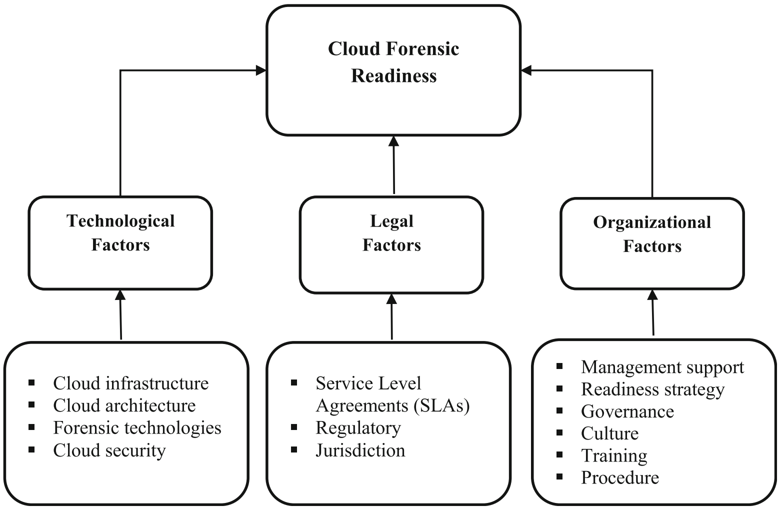

Fig. 2 The proposed cloud forensic readiness framework [15]

jurisdictions and regulatory issues. These factors are further elaborated below:

- **Service Level Agreements (SLAs)**: An SLA is a contract between a CSP and consumers that documents what services will be offered by the provider, including forensic investigations. SLAs should clearly specify the responsibilities of CSPs and customers associated with forensic investigations. Cloud providers and consumers need to agree on SLAs to avoid missing terms or conditions and to support potential digital investigations.
- **Regulatory**: This factor involves adherence to laws and regulations. To achieve forensic readiness, organizations must be aware of and comply with relevant laws, policies, and regulations. Moreover, cloud providers must adhere to the regulations imposed on service providers.
- **Jurisdiction**: This factor refers to the judicial region. Since CSPs may provide cloud services from different regions or areas, it is necessary for organizations to determine the judicial regions, if any, or to consider all multi-jurisdictions. It can be problematic for organizations to conduct an investigation while some data are not in the same jurisdiction or if multi-jurisdiction has not been specified in the service agreements. Furthermore, organizations should have a clear understanding of the legal and regulatory requirements of relevant jurisdictions. Organizations should agree with service providers regarding which jurisdictions data reside in and the cooperation during digital investigations.

Organizational factors

The organizational factors illustrate the characteristics of an organization and its employees that can facilitate cloud forensic readiness. These factors, defined below, have been highlighted by some research studies in the literature:

- **Management support**: This factor involves the top management level of the organization, which helps the organization achieve forensic readiness, including authorization, decision-making, necessary resources, and funds. It is important that the top management in organizations is aware of the importance of being forensically ready and has an influence on the establishment and implementation of the readiness of digital investigations.
- **Readiness strategy**: This factor is an organization's plan to achieve forensic readiness. In general, the strategy pertains to how the readiness would work. To achieve successful forensic readiness, organizations must clearly form dedicated strategic objectives that serve the organization's needs. The organization's readiness strategy must be flexible to adapt to potential changes.
- **Governance**: This factor refers to the management of the implementation of processes and structures in the organization that designate responsibilities and practices. This aspect includes the organization's general policy on cloud forensic readiness, such as managing forensics procedures and responsibilities related to digital evidence that is found in the cloud or any other resources. Ensuring that all procedures and responsibilities are structured in a correct way leads to a successful forensic investigation. In addition, governance can ensure the quality of forensic readiness in an organization.
- **Culture**: This factor concerns the pattern of beliefs, values, assumptions and practices that have a direct impact on cloud forensic readiness. Successful forensic readiness can be achieved by making a cultural change in relation to the importance of forensic readiness and a culture of adherence to best practices in relation to forensic readiness. This cultural change can be achieved through the implementation of staff training and awareness as well as forensics policies.
- **Training**: This factor involves providing training programmes to technical staff and awareness programmes to non-technical staff on forensics best practices. To achieve forensic readiness, organizations should educate and certify their technical staff through forensics training programmes to ensure that their skills and knowledge are up to date. Moreover, awareness training programmes should be provided to non-technical staff so that they know how to respond in the case of suspicious activities; indeed, such knowledge will minimize the risk of evidence loss.
- **Procedures**: This factor involves the organization's general policies on cloud forensics as well as security and privacy policies during digital investigations. Organizations should clearly state their forensics polices, as doing so will make it possible to collect admissible evidence. Such policies include various procedures, guidelines and standards that steer the digital investigation within an organization. The policies of the organization should be assessed periodically. Table 1 maps the identified factors to the literature [15].

Table 1 Mapping the identified factors to the literature [15].

Study	Forensic Readiness Factors												
	Technological Factors				Legal Factors			Organizational Factors					
	Infrastructure	Architecture	Technologies	Security	SLA	Regulatory	Jurisdiction	Management support	Strategy	Governance	Culture	Training	procedure
[16]	√		√			√	√			√	√	√	√
[18]		√	√			√		√		√	√	√	
[19]	√	√	√			√		√		√	√	√	
[24]	√		√	√									
[25]			√		√		√		√				√
[27]		√	√	√			√						
[21]			√	√		√	√		√	√		√	√
[29]	√		√	√		√	√		√				
[46]												√	√
[47]		√		√	√	√	√						√
[48]			√		√		√						√
[49]		√		√			√						√

Research methodology

When the nature of research is exploratory, a qualitative method is most suitable; such a methodology is employed to identify the perception of the audience under study in regard to certain issues [33]. The purpose of a qualitative approach is to clarify respondents' thoughts, feelings, decisions and actions [34]. In this way, it is possible to understand a certain situation, as a qualitative approach provides insights into issues that could well be the focus of future studies. Scholars often employ qualitative methods when working with the results of a literature review [35]. Because a qualitative approach generates a great deal of data, coding is the most commonly used approach to analysing data [33]. To identify and report the themes running through the raw data, thematic analysis was employed. Thematic analysis is a technique that makes it possible to collate and summarize a corpus in a particular way, which, in turn, aids researchers in locating vital elements that will allow them to produce effective research questions [36, 37]. To complete the analysis of the qualitative data, NVivo 11 software was employed to examine the themes of the raw data.

For this study, interviews were considered the most suitable approach for qualitative data collection [38]. Not only does this technique help researchers paint a comprehensive picture of the research topic, but it also makes it possible to validate and confirm the results. This study involved interviews with experts in the relevant field to review and verify the proposed framework. The interviews also made it possible to examine other factors that had not previously been mentioned in the framework. When employing this method, it was essential to link and contrast the data that resulted from the literature review, as well as the expert reviews. The first phase involved gathering data by analysing the literature and the relevant industry standards to construct a framework. During the expert interviews (second phase), the respondents were asked both open- and closed-ended questions to verify the framework and to add new factors not found within the framework.

In qualitative studies, the sample usually consists of fewer participants than in quantitative studies [39]. It is vital for researchers to clarify the minimum sample needed; in this way, pinpoint, reliable results can be obtained [40]. Scholars have yet to produce an agreed-upon consensus regarding how many experts should be interviewed when conducting a confirmatory study. The majority of research has recommended that between 3 and 20 experts should be interviewed [41]. However, Guest et al. [42] suggested that the saturation point is generally reached when 12 respondents are interviewed. As a result, the present study conducted interviews with 12 experts in the fields of security and digital forensics and who had experience in a cloud environment. The interviewees were deemed to be expert only if they had been working in the field of digital forensics and/or security for a minimum of five years, had worked with the IaaS model and/or made a contribution to this field. This study was set in various countries, as clearly shown in Table 2: Summary of the interviewees.:

Study findings

This section presents the findings from the expert reviews. Experts were interviewed to verify the proposed framework and to identify any factors that were not mentioned in the framework. The purpose

Table 2 Summary of the interviewees

Expert	Job Description	Years of Experience	Country
A	Cyber security and forensics expert	10+	UK
B	Cloud consultant	5	Saudi Arabia
C	Cloud security expert	6–10	USA
D	Senior manager of cyber investigations, eForensics, and digital development capabilities	6–10	UK
E	Security and digital forensics expert	10+	South Africa
F	Cloud forensics expert	6–10	Ireland
G	Cloud forensics expert	6–10	Australia
H	Digital forensics and cloud security expert	10+	Saudi Arabia
I	Cloud forensics expert	6–10	UAE
J	Cloud forensics expert	6–10	South Africa
K	Cloud and IoT forensics expert	5	Malaysia
L	Cloud forensics researcher	6–10	China

of the interviews was to seek out and clarify any problems related to cloud forensics and to assess how important it is for organizations to be ready to conduct digital investigations in cloud environments. The experts' opinions and comments are presented below:

Technological factors

The participants were asked to give their thoughts on the factors related to technological cloud forensic readiness. The interview results were clear: All experts were in agreement that the technological factors are very important or important in the context of cloud forensic readiness. Of the experts interviewed, most agreed that the infrastructure of the cloud is important in terms of achieving cloud forensic readiness. Additionally, every single expert stated that the architecture of the cloud is vital to achieving cloud forensic readiness. Moreover, all experts agreed that digital investigations cannot be conducted without forensics technologies that are able to produce reliable evidence. Similarly, all of the interviewed experts agreed that security during digital investigations is vital to achieving cloud forensic readiness. Table 3 presents some of the most notable findings in this regard.

Legal factors

Following the interviews, it was clear that the legal factors are important in relation to cloud forensic readiness. There was a clear agreement between the expert respondents regarding the importance of SLAs in cloud forensics. Additionally, most of the interviewees were in agreement regarding the importance of taking into account regulatory compliance with regard to achieving cloud forensic readiness. Six of the experts stated the opinion that the regulatory factor should to be changed to regulatory compliance. Moreover, many of the interviewees emphasized the importance of identifying the legal jurisdiction(s) before conducting digital investigations. Seven of the expert respondents opined that the jurisdiction factor

Table 3 Expert reviews of the technological factors

Factor	Expert	Comment
Cloud infrastructure	*C*	*"In order to facilitate potential digital investigations and be forensically ready, organizations should prepare the underlying infrastructure to support digital forensics".*
	B	*"Infrastructure has a direct impact on forensic readiness, so cloud infrastructure should correspond to digital forensics requirements".*
	H	*"It is important to prepare the infrastructure, but it is very difficult to amend it to fulfil forensics requirements".*
	I	*"Historically, security and forensics by design have proved to be efficient and necessary approaches to provide sound forensics services".*
	F	*"This is important to consider because of the chain of custody: it's necessary to trace every location of evidence".*
Cloud architecture	*B*	*"Excellent architecture means excellent readiness for forensics".*
	D	*"Correct architecture is required, as the digital forensic operator may not be involved and this piece is provided by the relevant ICT structure within the organization".*
	C	*"Cloud architecture is required to facilitate extra information (e.g., logs, flows) to corroborate findings".*
	J	*"The architecture has to support the running of processes".*
	K	*"Correct architecture is important, as it standardizes the data flow, which means that it is far easier to track and retrieve".*
Forensic technologies	*C*	*"Although a good analyst can make do with existing tools, up-to-date forensics technologies are very important".*
	J	*"The type of technology we choose determines if we can get credible evidence or not".*
	K	*"Without cutting-edge gadgets, the forensics process is going to be difficult to conduct".*
	E	*"I believe that forensic technologies are very important since those technologies will be the enablers of cloud forensic readiness".*
	I	*"Given the distributed nature and massive computing technology, forensics technologies need to be designed in a way that takes advantage of the computing power and encapsulates intelligence to serve forensic acquisition, examination and analysis".*
Cloud security	*B*	*"Security is a very important part, specifically for a forensics team, as it can provide them with a secure environment in which to conduct their investigation".*
	E	*"Obviously, security is still important because security measures are often more proactive than digital forensics measures".*
	C	*"Security helps eliminate false positives if properly configured, understood, and monitored".*
	H	*"Forensics and security bodies need to work together to gather evidence in a secure and forensic manner".*
	G	*"When security and forensics teams work together, it can assist in evidence correlation and integration between incident handling and digital forensics practices".*

should be changed to multi-jurisdictions. Table 4 presents a collection of some of the most notable statements made in this regard.

Organizational factors

As clearly shown by the findings from the expert interviews, the organizational factors are viewed as being very important or important in regard to achieving forensic readiness. It was fairly clear that a consensus existed among the respondents regarding the importance of management support in regard to achieving cloud forensic readiness. Moreover, all the interviewees agreed that if forensic readiness is to be achieved by organizations, then a readiness plan should be in place. Additionally, many of the interviewees pointed to the importance of organizational culture in regard to an organization reaching its goal of forensic readiness. Of all the experts interviewed, six felt that the culture factor should be replaced by the term organizational culture. Furthermore, the firm belief among all interviewees was that training is vital in regard to reaching forensic readiness within organizations; however, five interviewees opined that the training factor should instead be named training and awareness. Notably, all interviewees agreed that an organization has a better chance of achieving forensic readiness if it has digital forensics policies in place. In total, five of the interviewees suggested that the procedure factor should be changed to policies because policies would be a broader term that covers the various forensics procedures, guidelines and standards that steer digital investigations within an organization. The most notable statements made in this regard are presented in Table 5.

Overall, the proposed framework has been verified by the experts. Some of the proposed factors were altered, and new factors were added by the experts to improve the framework. The next section provides a discussion of the study findings.

Table 4 Expert reviews of the legal factors

Factor	Expert	Comment
Service Level Agreements (SLAs)	*A*	*“This is one of the main issues these days, as cloud forensics are considered afterwards – guidelines on to what extent a provider will assist with or take ownership of issues”.*
	J	*“Readiness involves mainly monitoring and collecting personal information. It is important to have an agreement prior to implementing this aspect”.*
	K	*“As the cloud is shared between consumers and providers, SLAs form a critical part when it comes to stating the roles and responsibilities of each party”.*
	D	*“We need to be able to obtain the digital evidence; if we are not able to do so, then we may not be able to fully investigate the crime. If we do have SLAs that include forensics scenarios, then we have the evidential requirement to support the investigation”.*
	I	*“The geographical separation between clients and the CSP is one of the main challenges in defining SLAs. SLA assessment and standardization might be needed to preserve the digital data in a forensically sound manner and to preserve the rights of both the CSP and clients. Enhancing SLAs definitely needs to be considered in the readiness framework”.*
	E	*“It is not crucial but very important to have SLAs in place because the proactive nature of cloud forensic readiness might impede the productivity of a system due to the additional overhead that cloud forensic readiness is prone to exhibiting”.*
Regulatory	*A*	*“Regulatory compliance is a very important factor to consider in this framework; organizations and CSPs need to comply with laws and regulations to avoid regulatory and financial consequences”.*
	L	*“The absence of regulations produces many different explanations for the same matter, while in these situations, consumers are the big loser”.*
	D	*“If we do not follow the regulatory codes or ISO or others, then potentially our evidence will not be available in the criminal justice process”.*
Jurisdiction	*F*	*“The physical borders in the cloud are not clear, so it is necessary for possible perimeters and related laws to be drawn or proposed”.*
	J	*“Though each jurisdiction varies, this is an important aspect in ensuring that crimes are prosecuted per the jurisdiction”.*
	E	*“Multi-jurisdiction is very important to consider in cloud forensics because the nature of public clouds often spans multiple jurisdictions, which may have different laws. However, it is not absolutely crucial because I think most organizations are focused on their own jurisdictions with some disregard for others”.*
	I	*“The geographical separation between clients and the CSP is one of the main challenges in cloud forensics. Multi-jurisdiction assessment and standardization might be needed to preserve the digital data in a forensically sound manner and to preserve the rights of both the CSP and clients. Multi-jurisdiction definitely needs to be considered in the readiness framework”.*

Table 5 Expert reviews of the organizational factors

Factor	Expert	Comment
Management support	*B*	*"Lack of management support causes a delay in or a failure to achieve the readiness".*
	D	*"There needs to be a good understanding and buy-in by the whole management team and organization".*
	C	*"Organizations cannot move to or adopt new technologies without support from the business".*
	K	*"It is very hard to have a well-qualified armed forensics team without endless support from the superiors and decision makers in the organization".*
	H	*"The readiness needs investment (money) and support (decision) from the top management".*
	I	*"Management is mostly business oriented, delivering investigators' points of view (and, in particular, readiness). Convincing stakeholders might require a great deal of effort".*
	E	*"This is very important because if an organization does not have buy-in from management, there will not be a sufficient budget (if any) assigned for CFR, and then, CFR will be non-existent".*
Readiness strategy	*D*	*"We need a clear plan about what the problem is, how we aim to achieve this, and the outcomes should be clearly defined".*
	E	*"Since strategy is a very proactive paradigm, it ties in directly with the paradigm of cloud forensic readiness, and that is to be proactive".*
	J	*"Without a strategy, implementation would be in jeopardy".*
	H	*"Success in the strategy resulted in success in forensics investigations and verse versa".*
Governance	*D*	*"We need a clear and well-defined governance structure, which should be simple, whilst covering all of the policies and procedures so as to ensure the integrity of the digital evidence obtained".*
	F	*"Every identified role must be carefully assigned, while specific duties should be introduced".*
	K	*"Governance is important in forensic readiness because it makes the forensics investigation team very systematic during their tasks and procedures, which can assure us that we are forensically ready".*
Culture	*I*	*"The changing mindset of CEOs, management and employees is a challenge that needs to be considered. On the other hand, the forensic investigators and analysts might show resistance in adopting the readiness framework".*
	D	*"There needs to be a good culture in policing attitudes regarding the correct ways to obtain, process and store digital evidence".*
	E	*"It is important to bring culture in since that automatically raises more awareness amongst the participants in the organization".*
Training	*K*	*"Training your staff is the first step towards being ready and armed against any cyberattack".*
	J	*"Training is a very important aspect of forensics. Each individual must know why the process is needed in an organization".*
	D	*"The correct training needs to be identified at the provided level within the organization, from the first responder through to the digital analyst".*
	E	*"I think training is less important to the organization as a whole but quite important in terms of digital forensic examiners. In addition, non-forensic teams need to be provided with awareness programmes on how to respond in the case of cyberattacks. This can help forensics teams to reduce the risk of evidence loss"*
	I	*"The fear of adopting new approaches, procedures and strategies can be considered the main obstacle. Training might be extremely helpful for families and shareholders with the new procedures or tools, and hence, it is very important".*
Procedure	*B*	*"Policies are very important for forensic readiness, as we can make sure that everything goes in the same direction and avoid self-interpretation".*
	D	*"You cannot operate in the digital forensics world at an evidentiary standard without good policy and procedures, both quality standards and technical standards. They go together".*
	L	*"I believe forensics policies are a set of rules that can guide people on what to do and what not to do before, during and after digital investigations, and this must be done by the senior management".*
	I	*"Forensics policies are important, as the current trend shows that, at both the national and international levels, efforts have been initiated towards a cloud, big data, and other evolving technology procedures".*

Discussion

The interviews with the experts verify the proposed framework; the names of five of the factors were altered, while two more factors were added, as can be seen in Fig. 3. As a result, following the literature review, the expert review and the questionnaire, the framework was verified. The following section examines the results of the expert reviews.

As stated in the literature [1, 6, 7, 43–45] and by a number of the interviewed experts, cloud computing has given rise to numerous issues and problems in the field of digital forensics. Indeed, any organization that uses cloud services must have a plan in place and pay attention to cloud forensics before future attacks happen. All experts agreed that forensic readiness is affected by the three dimensions, namely, legal, technological, and organizational factors. In addition, most of the experts agreed with the factors and saw no convincing reason to exclude any of the proposed factors. The findings of the interviews made it clear that the experts viewed these factors as important and felt that they have a substantial influence on cloud forensic readiness.

Following the interviews, it was also clear that all of the technological factors are vital in regard to achieving cloud forensic readiness. Moreover, a number of the experts asked for the inclusion of forensics techniques within the technological factors. With regard to the legal factors, most of the experts concurred with the factors proposed but felt that certain factors should be renamed, e.g., regulatory compliance instead of regulatory and multi-jurisdictional instead of jurisdiction. In addition, numerous experts expressed the feeling that the privacy factor should be added to the legal factors. Moreover, the experts stated that all of the organizational factors are vital, with none of them recommending that new factors needed to be added. Nevertheless, certain experts suggested that a few factors should be renamed. The procedure factor has been renamed policies. Given the significant influence of cloud forensics on the standardization process and its need, the term policies would be a wider term that includes the forensics procedures, guidelines and standards that guide digital investigations within an organization. While cloud computing poses a number of digital forensics challenges, there are no specially designed guidelines, procedures or standards pertaining to cloud forensics [6]. Consequently, we would like to take this opportunity to argue that standard-setting bodies need to establish policies, guidelines and standards dedicated to the cloud computing environment.

Moreover, the culture factor has been changed to organizational culture to focus on the practices that have a direct impact on the forensic readiness in organizations. The training and awareness factor has replaced training. This process involves technical and non-technical staff by providing training programmes to technical staff and awareness programmes to non-technical staff on forensics best practices.

However, it was also important for the experts to improve the proposed framework by adding any essential factors that were not stated in the framework and that could potentially affect cloud forensic readiness within organizations. In reference to this point, the experts identified two new factors – namely, privacy and forensics techniques – which they thought should be taken into account by organizations that are preparing for forensic readiness. Both of these factors were viewed as important; indeed, five experts felt that they should be included in the framework. They also stated that it is vital to add the privacy factor to the legal factors of the proposed framework. The experts in digital forensics defined privacy as the retention of information and data that are accessed, gathered, logged, and wiped throughout and after investigations related to digital forensics. All the experts expressed the belief that organizations should have proper mechanisms to ensure privacy during a forensic investigation. No previous study has emphasized privacy during digital investigations in their proposed solutions. Subsequently, the

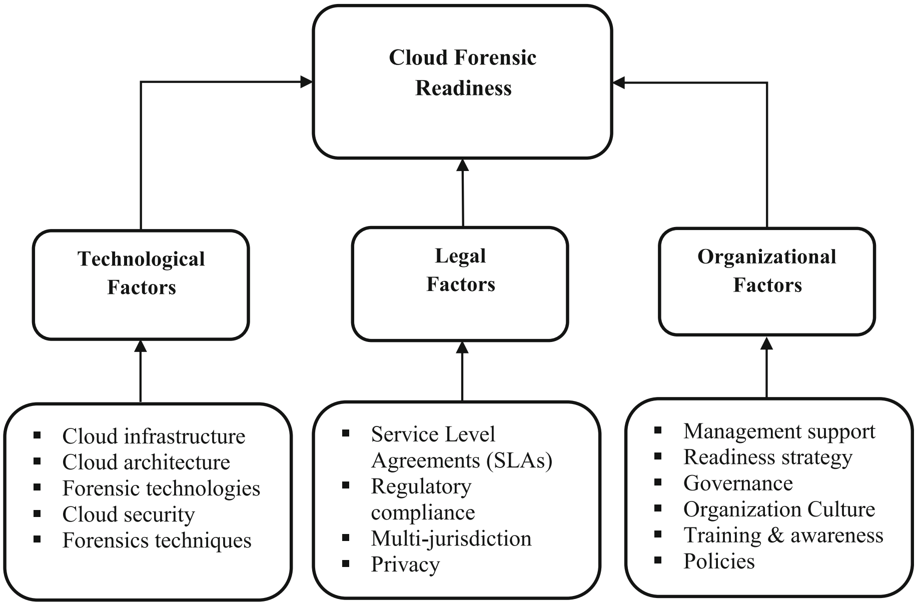

Fig. 3 The verified cloud forensic readiness framework

decision was made to add the privacy factor to the legal factors category.

In addition, seven of the experts suggested that a new factor, designated forensics techniques, should be added to the technological factors. Forensics techniques are employed when there is a need to respond to and to conduct investigations into cloud forensics within an organization. Such forensics techniques may include those used to provide answers to the "5 W" questions: What happened? When did it happen? Where did it happen? Why did it happen? Who did it? Following this, the focus switches to summarizing the investigation's results (e.g., the first reaction, data acquisition, data assessment and evaluation, and conclusions). These techniques allow organizations to collect evidence such that means it can be used as admissible evidence in a court of law. These types of measures aid organizations in minimizing the possibility that their business will be interrupted. Accordingly, it was decided that the forensics techniques factor should be included in the technological factors category.

It should be noted at this point that numerous other factors were mentioned but ignored because they were already covered in the framework. These omitted factors included the handling of forensic evidence, which overlaps with forensics techniques, and qualifications, which overlap with training and awareness.

Conclusions

Although cloud environments are now an alluring environment for cybercrime, there remains precious little research that has addressed forensic readiness in cloud environments. This paper started by providing an overview of digital forensics and then discussed the related work. From the literature review, it was clear that it is essential to explore forensic readiness in cloud environments. Therefore, this study aimed to investigate the cloud forensic readiness factors that influence organizations to be prepared to conduct cloud forensic investigations. In this paper, the proposed framework was reviewed and verified by a number of experts in the fields of security and digital forensics. In terms of the results of the expert reviews, it was clear that all the proposed dimensions and factors are important. Five factors were renamed, and two new factors were added by the experts. In future work, a survey will be distributed to cloud forensics practitioners in different organizations to validate the cloud forensic readiness framework. Doing so will help us construct an instrument derived from the verified framework to measure organizations' forensic readiness status.

Abbreviations

CAGR: global compound annual growth; CPCS: Cyber-Physical Cloud Systems; CSPs: Cloud Service Providers; DFIRP: Digital Forensic Investigation Readiness Process; IaaS: Infrastructure as a Service; ISO/IEC: International Organization for Standardization/International Electrotechnical Commission; IT: Information Technology; NIST: The National Institute of Standards and Technology; SLAs: Service Level Agreements

Acknowledgements

We acknowledge Northern Borders University in Saudi Arabia and the Saudi Arabian Cultural Bureau in the UK for their scholarship to Ahmed Alenezi that allows the research to be funded and undertaken.

Authors' contributions

AA designed and developed the proposed framework as well as confirmed the framework by interviewing number of experts. HA has been involved in drafting the manuscript, while GW contributed to the abstract part and supervised AA. All authors read and approved the final manuscript.

Authors information

Ahmed Alenezi a lecturer at Northern Border University, Saudi Arabia and a Ph.D. candidate at the University of Southampton, UK. Ahmed is interested in multidisciplinary research topics that related to computer science. His research interests include and not limited to: Parallel Computing, Digital forensics, Cloud Forensics, Cloud Security, Internet of Things Forensics and Internet of Things Security. Ahmed's Ph.D. research project focuses on Cloud Forensics.

Hany F. Atlam has large experiences in networking as he holds international Cisco certifications, Cisco Instructor certifications, and database certifications. Hany's research areas include IoT security and privacy, Cloud computing security, Blockchain, Big data, digital forensics, computer networking and image processing.

Gary Wills is an Associate Professor in Computer Science at the University of Southampton. He graduated from the University of Southampton with an Honours degree in Electromechanical Engineering, and then a PhD in Industrial Hypermedia systems. He is a Chartered Engineer, a member of the Institute of Engineering Technology and a Principal Fellow of the Higher Educational Academy. He is also a visiting associate professor at the University of Cape Town and a research professor at RLabs. Gary's research projects focus on Secure System Engineering and applications for industry, medicine and education.

Funding

The research is funded by Northern Border University, Saudi Arabia.

Availability of data and materials

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Received: 24 October 2018 Accepted: 27 June 2019
Published online: 14 August 2019

References

1. Ruan K, Carthy J, Kechadi T, Crosbie M (2011) Cloud forensics. An Overview IFIP Conference on Digital Forensics:35–46. https://doi.org/10.1007/978-3-642-24212-03
2. Buyya R, Yeo CS, Venugopal S et al (2009) Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Futur Gener Comput Syst 25:599–616. https://doi.org/10.1016/j.future.2008.12.001
3. Armbrust M, Stoica I, Zaharia M et al (2010) A view of cloud computing. Commun ACM 53:50. https://doi.org/10.1145/1721654.1721672
4. Marco L De, Kechadi M-T, Ferrucci F (2013) Cloud Forensic Readiness: Foundations. International Conference on Digital Forensics and Cyber Crime 237–244
5. Market Research Media. In: Market research media. 2016. http://www.marketresearchmedia.com/?p=839 . Accessed 16 July 2017.
6. Sang T (2013) A log-based approach to make digital forensics easier on cloud computing. Proceedings of the 2013 3rd international conference on

intelligent system design and engineering applications, ISDEA 2013 91–94. https://doi.org/10.1109/ISDEA.2012.29

7. NIST (2014) NIST Cloud Computing Forensic Science Challenges
8. Kent K, Chevalier S, Grance T, Dang H (2006) Guide to integrating forensic techniques into incident response. NIST Special Publication
9. Palmer G (2001) A road map for digital forensic research. First digital forensic research workshop 1–42. https://doi.org/10.1111/j.1365-2656.2005.01025.x
10. Raghavan S (2013) Digital forensic research: current state of the art. CSI Transactions on ICT 1:91–114. https://doi.org/10.1007/s40012-012-0008-7
11. Hewling M (2013) Digital forensics: an integrated approach for the Investigation of Cyber/Computer Related Crimes
12. Yung Chou (2010) Cloud Computing for IT Pros (2/6): What Is Cloud. https://blogs.technet.microsoft.com/yungchou/2010/12/17/cloud-computing-for-it-pros-26-what-is-cloud/. Accessed 19 Mar 2019
13. Zawoad S, Hasan R (2013) Digital forensics in the cloud. The Journal of Defense Software Engineering (Cross Talk) 26:17–20
14. Pangalos G, Katos V (2010) Information assurance and forensic readiness. In: International conference on e-democracy. Springer, Berlin Heidelberg, pp 181–188
15. Alenezi A, Hussein RK, Walters RJ, Wills GB (2017) A framework for cloud forensic readiness in organizations. In: 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud) pp 199–204
16. Grobler CP, Louwrens CP, Von Solms SH (2010) A framework to guide the implementation of proactive digital forensics in organizations. Availability, reliability, and security, 2010 ARES '10 international conference 677–682. https://doi.org/10.1109/ARES.2010.62
17. Alharbi S, Weber-Jahnke J, Traore I (2011) The proactive and reactive digital forensics investigation process: a systematic literature review. International Journal of Security and Its Applications 5:59–72. https://doi.org/10.1007/978-3-642-23141-4
18. Elyas M, Maynard SB, Ahmad A, Lonie A (2014) Towards a systematic framework for digital forensic readiness. J Comput Inf Syst 54:97–105. https://doi.org/10.1108/17506200710779521
19. Elyas M, Ahmad A, Maynard SB, Lonie A (2015) Digital forensic readiness: expert perspectives on a theoretical framework. Computers and Security 52:70–89. https://doi.org/10.1016/j.cose.2015.04.003
20. Valjarevic A, Venter H (2013) Implementation guidelines for a harmonised digital forensic investigation readiness process model. 2013 Information Security for South Africa 1–9.
21. Moussa AN, Ithnin NB, Miaikil OA. (2014) Conceptual forensic readiness framework for infrastructure as a service consumers. In: Systems, Process and Control (ICSPC), 2014 IEEE Conference pp 162–167.
22. Simou S, Troumpis I, Kalloniatis C et al (2018) A decision-making approach for improving organizations' cloud forensic readiness. In: International conference on trust and privacy in digital business, pp 150–164
23. Park S, Kim Y, Park G et al (2018) Research on digital forensic readiness Design in a Cloud Computing-Based Smart Work Environment. Sustainability 4:1–24
24. Sibiya G, Fogwill T, Venter HS, Ngobeni S (2013) Digital forensic readiness in a cloud environment. AFRICON, IEEE:1–5
25. Makutsoane MP, Leonard A (2014) A conceptual framework to determine the digital forensic readiness of a cloud service provider. In: Proceedings of PICMET '14 conference. Portland International Center for Management of Engineering and Technology; Infrastructure and Service Integration, pp 3313–3321
26. Kebande VR, Venter HS (2014) A cloud forensic readiness model using a botnet as a service. The international conference on digital security and forensics (DigitalSec2014) 23–32
27. Kebande VR, Venter HS (2016) Requirements for achieving digital forensic readiness in the cloud environment using an NMB solution. 11th International Conference on Cyber Warfare and Security ICCWS
28. Kebande VR, Venter HS (2017) Novel digital forensic readiness technique in the cloud environment. Australian Journal of Forensic Sciences 50:552–591. https://doi.org/10.1080/00450618.2016.1267797
29. Ab Rahman NH, Glisson WB, Yang Y, Choo K-KR (2016) Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Computing 3:50–59
30. Dykstra J, Sherman AT (2012) Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques. Digit Investig 9:S90–S98
31. Trenwith PM, Venter HS (2013) Digital forensic readiness in the cloud. 2013 Information Security for South Africa IEEE.
32. Zawoad S, Dutta AK, Hasan R (2013) SecLaaS: secure logging-as-a-service for cloud forensics. In: the 8th ACM SIGSAC symposium on Information, computer and communications security. pp 219–230.
33. J w C (2009) Research design: Qualitative, quantitative, And mixed methods approaches
34. Creswell JW, Clark VLP (2007) Designing and conducting mixed methods research
35. Fink A (2003) The survey handbook
36. Aronson J (1995) A pragmatic view of thematic analysis. In: The qualitative report
37. Braun V, Clarke V (2006) Using thematic analysis in psychology. Qualitative research in psychology.
38. Sekaran U (2000) Research methods for business. John Wiley & Sons, Inc
39. Hancock B, Ockleford E, Windridge K (1998) An introduction to qualitative research.
40. Banerjee A, Chitnis U, Jadhav S (2009) Hypothesis testing, type I and type II errors. Industrial psychiatry.
41. Grant J, Davis L (1997) Selection and use of content experts for instrument development. Research in nursing & health.
42. Guest G, Bunce A, Johnson L (2006) How many interviews are enough ? An experiment with data saturation and variability. Family Health International 18:59–82. https://doi.org/10.1177/1525822X05279903
43. Zargari S, Benford D (2012) Cloud forensics: concepts, issues, and challenges. Third International Conference on Emerging Intelligent Data and Web Technologies:236–243
44. Choo KR, Antonio S, Choo R (2017) Evidence and forensics in the cloud: challenges and future research directions. IEEE Cloud Computing 4:14–19
45. Pichan A, Lazarescu M, Soh ST (2015) Cloud forensics: technical challenges, solutions and comparative analysis. Digit Investig:38–57. https://doi.org/10.1016/j.diin.2015.03.002
46. ACPO (2012) ACPO Good practice Guide for Digital Evidence.
47. CSA (2013) Mapping the forensic standard ISO / IEC 27037 to cloud computing. Cloud Security Alliance:1–31
48. Liveri D, Skouloudi C (2016) Exploring Cloud Incidents. The European Network and Information Security Agency (ENISA) 1–14.
49. ISO/IEC-27043 (2015) Information technology — security techniques — incident investigation principles and processes.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.