Cloud Forensics Investigations Relationship: A Model And Instrument

Full Paper

Younis AL Husaini
Deakin University Centre for Cyber Security Research and Innovation
Deakin University, Geelong, Victoria, Australia
Email: yalhusai@deakin.edu.au

Matthew Warren
Deakin University Centre for Cyber Security Research and Innovation
Deakin University, Geelong, Victoria, Australia
Email: matthew.warren@deakin.edu.au

Lei Pan
Deakin University Centre for Cyber Security Research and Innovation
Deakin University, Geelong, Victoria, Australia
Email: l.pan@deakin.edu.au

Mansoor AL Gharibi
Deakin University Centre for Cyber Security Research and Innovation
Deakin University, Geelong, Victoria, Australia
Email: malghari@deakin.edu.au

Abstract

Cloud computing is one of the most important advances in computing in recent history. cybercrime has developed side by side and rapidly in recent years. Previous studies had confirmed the existing gap between cloud service providers (CSPs) and law enforcement agencies (LEAs), and LEAs cannot work without the cooperation of CSPs. Their relationship is influenced by legal, organisational and technical dimensions, which affect the investigations. Therefore, it is essential to enhance the cloud forensics relationship between LEAs and CSPs. This research addresses the need for a unified collaborative model to facilitate proper investigations and explore and evaluate existing different models involved in the relationship between Omani LEAs and local CSPs as a participant in investigations. Further, it proposes a validated research instrument that can be cloud forensics survey. It can also be used as an evaluation tool to identify, measure, and manage cloud forensic investigations.

Keywords Cloud Forensics, Incident Response, Law Enforcement Agents, Cloud Service Providers, Cloud Forensics Readiness, construct, instrument, survey, reliability, validity.

1 INTRODUCTION

Cloud computing has become a revolution in the technology world, and both individuals and institutions are using cloud services and becoming dependent on it. By replacing old systems to cloud services, organisations can save time and cost (Al-Gharibi 2019b). Gartner expects cloud services to exceed $300 billion by 2021 (Gartner 2018). Governments are now turning to the application of cloud computing for the delivery of their systems and services. Due to this emerging technology, most of the current digital crime forensic cases have moved from local device storage to the cloud, including smart devices connected to cloud environments. The result of this change is seen in the daunting challenges that Law Enforcement faces when conducting investigations involving data stored in the cloud. Hence, Digital Forensics (DF) had a new specialisation named as "Cloud Forensics (CF)".

The challenges have become bigger for law enforcement with cloud forensics investigations, where LEAs cannot work without the cooperation of CSPs. The relationship between LEAs and CSPs is overwhelmed by many challenges, in the legal, organisational and technical levels, which negatively affect the cooperation between the two organisations (Al Husaini 2018b; Dykstra 2013; Liveri & Skouloudi 2016; NIST 2014; Ruan & Carthy 2012; Ruan et al. 2013; Ruan et al. 2011)

This problem is not trivial because LEAs cannot work without the cooperation of CSPs. Their relationship does not have one challenge that can be addressed solely by organisational level, in facts, the organisational, legal and technical challenges are interlinked. Based on the literature review, there is no previous studies on this relationship. For this reason, this study focuses on the current situation of cloud forensics in Oman as a case study and seek to understand the existing relationship between Omani LEAs and local CSPs by answering the research question: What are the factors that impact upon the relationship between Omani LEAs and local CSPs?

A survey is designed to contribute in answering the research question, this paper aims is to propose a validated research instrument for this survey. It can also be used as an evaluation tool to identify, measure, and manage cloud forensics investigations relationship. Implications of the study suggest a need for rigorous research to understand this relationship and how it affects the path of real-world digital forensic cases.

The remaining of this paper subsections cover a literature review of cloud, digital forensics, digital forensics in Oman and cloud forensics. In section two we introduce and discuss existing Cloud Forensics Readiness (CFR) models and relevant standards and, in section three we explore the conceptual framework and hypotheses. Section four discusses the research methodology, and finally, we share the result and conclusions.

1.1 Digital Forensics

The prime purpose of Digital Forensics is to facilitate the reconstruction of events and actions which are found to be criminal or helping to anticipate any malicious actions shown to be troublesome to planned operations. Therefore, the credibility of digital evidence is at the core of the digital forensic process because it is the means by which a forensic conclusion is either accepted or rejected (Selamat, Yusof & Sahib 2008).

Despite many assertions by researchers about the importance of an international standard for digital forensics (Al Husaini 2018a; Du, Le-Khac & Scanlon 2017; Kohn, Eloff & Eloff 2013; Reith, Carr & Gunsch 2002), there are several standards such as the ISO standards(ISO 27037 2012; ISO/27043 2015) academic, UK and US standards (UK: Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence(Williams 2012), US: “Electronic Crime Scene Investigation: A Guide for First Responders”(Ballou 2010))

However, these are generic guidelines to deal with digital evidence and each suggests different phases and processes, which leads to the different countries develop their own operational level to comply with local procedures, policies, and principles in a given country.

1.2 Digital Forensics in OMAN

Oman established the National Digital Forensics Lab (NDFL), which was opened in February 2016 (MuscatDaily 2016; Times_Of_Oman 2016). One year later in 2017, it obtained international accreditation by the ANSI-ASQ National Accreditation Board (ANAB). This laboratory is used to collect evidence and to assist LEAs and judicial authorities with investigating these crimes.

In Oman, more than 2,800 phone calls and over 420 e-mails were registered to report about cybercrimes by the end of 2016, which required the intervention of the NDFL. In 2017, the NDFL handled 172 DF

cases involving 877 evidence devices including computers, mobile, phones, external hard disk and USBs, which resulted from cybercrime cases in Oman (Ras & Venter 2015).

1.3 Cloud Computing

Cloud computing cannot be considered a new technological term, but just in 2007 only cloud computing was introduced to the public, after the announcement of Google and IBM cooperation in cloud technologies (A Vouk 2008; Alenezi et al. 2017). Gartner predicts cloud services around the world to grow in 2018 to more than $ 186 billion, an increase of 21.4 per cent from 2017, as it is expected to exceed $ 300 billion by 2021 (Gartner 2018). Cloud computing has been defended by NIST as “Model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell & Grance 2011).

Despite all the benefits of cloud computing, shifting to the cloud is a challenge and the cloud computing invite vulnerabilities that can be used in cybercrime (Al-Gharibi 2018). Although there are security risks involved, the public and private sectors have chosen to adopt cloud computing. For example, in government, they approach cloud services implementation. These include commercial cloud services, government cloud services developed by the government, and government cloud services developed by private companies (Al-Gharibi 2019a).

1.4 Cloud Forensics

Previous researchers have published numerous papers on cloud forensic with great interest in cloud computing. However, despite all this research, no solutions were found to address the cloud forensics challenges (Zhao & Duncan 2018).

Many researchers argue that the challenges of cloud forensics cannot be solved through technology alone because there are regulatory and legal principles that must be solved side by side (De Marco 2015). Numerous challenges that need to be solved in all these areas, many academic, technical, regulatory and legal researchers have begun to discuss these challenges, such as trustworthiness, acountablity, and Lack of international agreements & laws (Al Husaini 2018c; Liveri & Skouloudi 2016; Mell & Grance 2014).

The term of the cloud forensics is relatively new. The first researcher presented this term in 2011 (Ruan et al. 2011) (Alenezi et al. 2017), who introduced organisational, technical and legal cloud forensics challenges. NIST has defended cloud computing as "Cloud computing forensics science is 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" (Mell & Grance 2014).

2 PREVIOUS STUDIES

Cloud forensics readiness has been well studied by many researchers (Ab Rahman et al. 2016; Alenezi et al. 2017; Elyas et al. 2014; Grobler, Louwrens & von Solms 2010; ISO/27043 2015; Kebande & Venter 2014; Liveri & Skouloudi 2016; Makutsoane & Leonard 2014; Moussa, Ithnin & Miaikil 2014; NIST 2014; Sibiya et al. 2013; Trenwith & Venter 2013; Valjarevic & Venter 2013). A theoretical framework was proposed with some suggested technical solutions which will be reviewed below:

The NIST Cloud Computing Forensic Science Working Group (NCC FSWG)(Mell & Grance 2014) is one of the most critical reports that highlight the challenges and problems of cloud forensics. However, the report is relatively outdated, as the NCC FSWG has not issued any other report in this area, and it might be due to the lack of financial support for the group. Yet it is the most detailed and comprehensive comparison to other papers so far.

Another excellent report related to cloud forensic was published in 2016 by European Network and Information Security Agency (ENISA), which came under the title "Exploring Cloud Incidents" It provides an overview of the current state of cloud forensic and the incident response, and identifying and analysing the current technical, legislative, organisational challenges (Liveri & Skouloudi 2016).

One of the CFR models is of interest by implementing a Botnet solution for monitoring the cloud environment and providing acceptable digital evidence that can be used within the courts, which is proposed by (Kebande & Venter 2014), yet this model needed to be standardised to integrate with other cloud processes. Another forensics readiness model which could be used by CSPs as a technique for DFR,

which can help CSPs to control evidence is required for investigations. However the range of this framework is restricted to data examination in forensic analysis within the cloud infrastructure (Sibiya et al. 2013).

Remote access / central to the investigator to the cloud computing it was one of the proposed models for CFR by (Trenwith & Venter 2013), which could support digital forensics investigators to do their work.

A conceptual model for immigrating the organisations to the cloud environment suggested by (Makutsoane & Leonard 2014), the idea was to define the status of readiness of CSPs. The proposed model, which involves a process tool, allows organisations to create the right decision and choose the suitable CSP. Highlighting the requirements of cloud forensics, the authors used a non Malicious Botnet to measure forensic readiness. Those suggested requirements include technical, operational and legal aspects based on the (ISO/27043 2015) standard. Once again the requirements need to be ascertained and tested to ensure the performance is not only effective but can be a standard to which all forensic investigations are conducted and will continue to evolve with future technologies (Kebande & Venter 2016). A conceptual framework which is detected to help laaS users activate forensics readiness. The framework shows how IaaS users can get potential digital evidence without depending on CSPs. This model includes nine elements, containing the technical, legal and organisational forensics readiness core values (Moussa, Ithnin & Miaikil 2014).

A forensics-by-design framework for Cyber-Physical Cloud Systems (CPCS) suggested by (Ab Rahman et al. 2016), where they are highlighting the significance of forensic readiness. It contains six elements and assures us that a CPCS can be intended for facilitating forensic investigations. This framework can help investigators and accelerate forensic investigations. CFR framework by highlighting the factors affecting CFR technical, legal and regulatory (Alenezi et al. 2017).

According to the previous literature review, there are concerns and lack of confidence that the CSPs will be the first to respond to an incident. There is a consensus amongst researchers that there are gaps and conflict of interest between CSPs and LEAs.

In this study, we will highlight the relationship between LEAs and CSPs and classify the essential factors to be understood in order to enhance and organise the relationship.

3 CONCEPTUAL FRAMEWORK AND HYPOTHESES

There is a broad consensus among researchers (Almulla, Iraqi & Jones 2014; Alqahtany et al. 2017; Grispos, Storer & Glisson 2013; Liveri & Skouloudi 2016; Mell & Grance 2011; Ruan et al. 2011; Zhang, Wang & Han 2014) that the CSPs should cooperate with LEAs to make successful forensic investigations into cloud computing, as all powers are with the CSPs, and LEAs cannot operate without the cooperation of the CSPs. Although there is consensus on the importance of CSPs cooperation with LEAs, there is still no research study to highlight this relationship and identify the factors that need to be understood in order to enhance and streamline the relationship.

For effective cloud forensic investigations, three main dimensions consisting of seven factors were proposed as shown in Figure 1. These three dimensions are based on institutional theory, which is regulative, normative, and cognitive. A detailed discussion of the seven factors (trustworthiness, segregation of duties, standards, laws and regulations, readiness, accountability, technology compatibility) is also presented.

Figure 1 illustrates the overlap between the functions of LEAs and CSPs. We note the gap in the middle of the overlapped area. This gap has been confirmed by some researchers (Almulla, Iraqi & Jones 2014; Alqahtany et al. 2017; Grispos, Storer & Glisson 2013; Liveri & Skouloudi 2016; Ruan et al. 2011; Zhang, Wang & Han 2014).

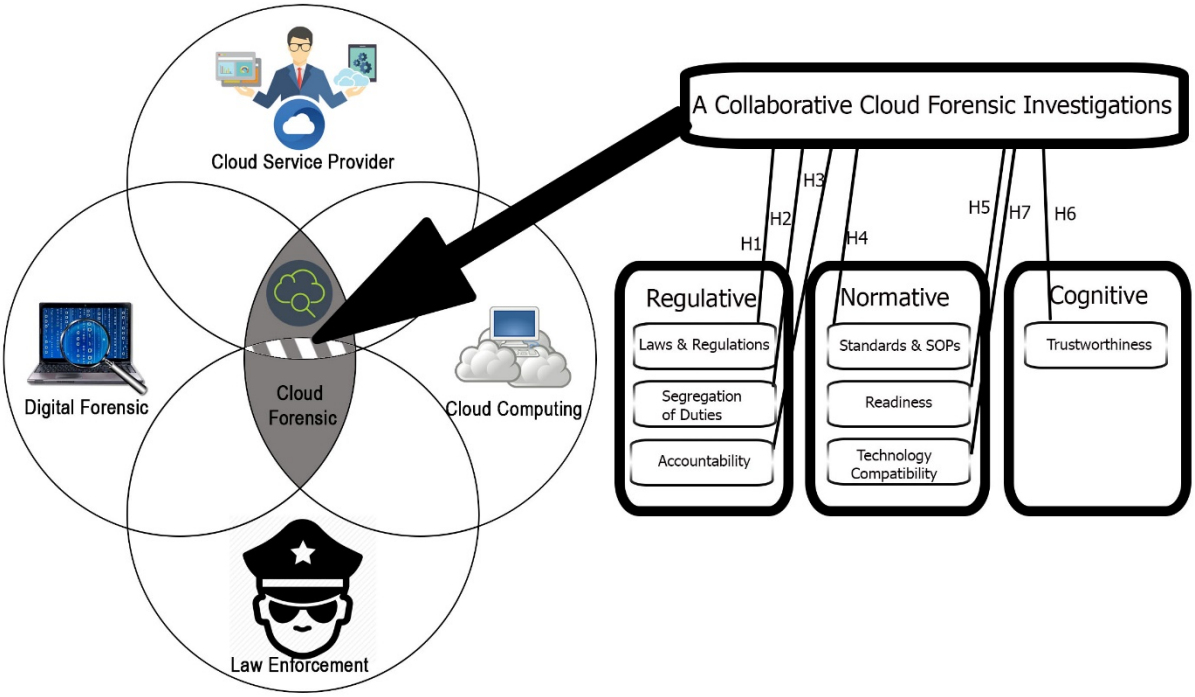

Figure 1 Conceptual Framework for a Collaborative Cloud Forensic Investigations

Figure 1 also shows a conceptual framework to analyse the critical factors for the relationship between CSPs and LEAs. There are seven hypotheses (H1-H7) as given below:

H1: Laws and regulations have a critical impact on the relationship between CSPs and LEAs.

H2: The segregation of duties has a critical impact on the relationship between CSPs and LEAs.

H3: Accountability has a critical impact on the relationship between CSPs and LEAs.

H4: The SOPs & Standards have a critical impact on the relationship between CSPs and LEAs.

H5: Readiness has a critical impact on the relationship between CSPs and LEAs.

H6: The trustworthiness of CSPs has a critical impact on the relationship between CSPs and LEAs.

H7: The technology compatibility of CSPs has a critical impact on the relationship with LEAs.

4 RESEARCH METHODOLOGY

For the experimental evaluation of the presented hypotheses and proposed model, we developed a survey instrument, which is to achieve the correctness and accuracy of the tool, and reduce the measurement error based on the previous guidelines that have been developed in the literature (Aladalah, Cheung & Lee 2016; Lewis, Templeton & Byrd 2005; MacKenzie, Podsakoff & Podsakoff 2011; Moore & Benbasat 1991).

This survey will help to test and confirm the factors suggested in the hypothesis. This will lead to understand relationship between the LEAs and CSPs. We validated the instrument as summarised in Table 1.

Phase	Description
Construct definition	Constructs definition were derived from a variety of sources including pre-existing definitions, and mostly prior relevant literature reviews.
Item generation	Scales were adopted from relevant literature when possible. Items were developed for other constructs Appendix 1.
Expertise Feedback	The draft survey was sent to academic and experts in the field, three senior academic and three amendments were made to the items. Four expertise from the industry, law enforcement agency and local cloud service providers.
Q-sorting	Qualtrics Q-sorting was used, where participants were asked to drag and drop random items inside boxes displaying factors. A two-stage examination was performed to improve reliability

Phase	Description
	and validity. Practical experience has been taken into account and it was that participants must not have less than 5 years of experience. Also, their educational level must not be less than master degree for practitioners, and a PhD for academics. Two academics with practical experience in digital forensics and two experts in digital forensics from industry, two practitioners at each stage, resulting in modifications in the formulation of several items (Appendix 1).
Pre-testing	To enhance reliability and validity, two academics completed the initial questionnaire. There was a slight change in length, structure, wording of the Questionnaire.
Pilot test	7 law enforcement agencies, cloud services providers, academics, professionals in the field finished the survey. There was a minor change were made based on their feedback.

Table 1. Instrument development process

4.1 Conceptualization and Operationalization

Following to the conceptual definition of the whole constructs, which has been operationalised using validated items from previous related studies. We then validated the measures and adjusted those items to fit the LEAs & CSPs relationship context. The scales have been developed for some items by following the development guidelines using the existing literature (Lewis, Templeton & Byrd 2005). In order to assure the validity and reliability of the instrument (Neuman 2011), and to verify that the participants have sufficiently understood the items, multi indicators have been used. Maintaining the short measure is effective to reduce the response bias caused by boredom or fatigue. Harvey, Billings and Nilan (1985) recommended to evaluate the homogeneity of items at each latent construct, which requires at least four items for each scale. The final survey consists of four items or more to all factors. The final measures are given in Appendix 1.

4.2 Q-sorting

Q-Sorting is one technique utilised to evaluate the reliability and validity of survey measurements developed for the questionnaire (Nahm et al. 2002). The goal of the Q-sorting is to test the items empirically to decide whether each item in the survey represents the corresponding factor (Lewis, Templeton & Byrd 2005). The method involves two different stages, each stage consisted of different pairs of judges. Two participants were digital forensics academics, other two were digital forensics experts from the industry. Participants were grouped in pairs, an academic and a practitioner in each round. Judges were not allowed to any cooperation among them. On the other hand, they have the right to ask anything relevant to the Q-sorting procedures (Brown 1996). To evaluate and assess the measurement validity and reliability, the inter-judge agreement level was calculated by Cohen's Kappa Index (Cohen 1960) and the hit ratio (Moore & Benbasat 1991), both have been used as evaluation criteria in order to evaluate the measurement reliability and validity. Regarding Kappa, there are no general agreement exists, but several scholars recommended the following: rates from (.76 -1.00) are considered to be excellent agreement, rates from (.40 - .75) are considered to be fair to moderate agreement, and rates from (.39 or less) are considered poor agreement (Landis & Koch 1977). According to hit ratio, the higher the percentage of items placed in the correct construct, the higher the degree of the inter-judge agreement occurred.

		Actual									
	Construct	1	2	3	4	5	6	7	N/A	Total	Hits
Theoretical	1	11			1	1			1	14	79%
	2	1	10			1	1		1	14	71%
	3			11	1		2			14	79%
	4			1	7					8	88%
	5	1				9	1		1	12	75%
	6	1					6		1	8	75%
	7	1						7		8	88%
	Total items placement:			78	Number of hits:		61		79%	Overall hit ratio:	

Table 2. First sorting stage

In the first stage, a pool of 39 items was presented randomly, and each judge was present with 7 factors and 39 items and was asked to drag and drop them into the factor boxes. "Not Applicable" box has been added to guarantee the judges' freedom to decide, thereby not pushing them into a particular box. In this round, two judges agreed on 32 out of 39 items; an average "hit ratio" of 79 percent was attained as 61 out of 78 items were correctly classified as shown in Table 2. The first sorting round resulted in a rewording of the ambiguous items, and also the deletion of undetermined items. Exactly 3 items have been deleted, and 6 items have been reworded. Table 3 presents the round 2 of the Q-sorting.

		Actual									
	Construct	1	2	3	4	5	6	7	N/A	Total	Hits
Theoretical	1	10								10	100%
	2	1	13							14	93%
	3			10	1				1	12	90%
	4			1	7					8	88%
	5					9	1			10	90%
	6						8			8	100%
	7							8		8	100%
	Total items placement:			70	Number of hits:		65		93%	Overall hit ratio:	

Table 3. Second sorting stage

The phase two of Q-sorting presented 35 items for the constructs. Two judges agreed on 33 out of the 35 items with a hit ratio of 93 percent, almost 14 percentage improvement compared to phase one, as 65 of 70 items were accurately categorised as shown in Table 3. Whereas, the calculated Kappas yielded values is above 0.90. Following Landis and Koch (1977) guidelines for acceptable levels for Cohen's Kappa Index, which is considered above 0.76 as an excellent agreement level, we decided to end the Q-Sorting, with average placement ratio of 93%, which confirmed a high level of reliability and construct validity. Overall, the methods utilised are deemed as adequate in meeting the content validity, and the instrument is ready for the next phase.

4.3 Pilot test

The goal of this phase is to evaluate the items and the general format. As the final sample for this research is limited to Omani expertise in the field, this phase involved 8 digital forensics expertise, cloud servers providers and academics researchers. Pilot test participants were asked to fill the survey and then gives feedback on the level of difficulty in completing the survey. The survey investigated the proposed model constructs on a 5 point Likert (1932) started from 'Very Important' to 'Not at all important'. Moreover, the pilot test participants have been asked to gives their suggestions for any improvement. The final outcome of this phase has improved the quality of the survey, and presented to the final draft of the survey.

5 ANALYSIS AND RESULTS

5.1 Initial reliability

In order to evaluate the initial reliability of the instrument, we calculate the Barlett's Test of Sphericity and Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy. The correlation matrix unveiled the presence of several coefficients as 0.3 and above. This was considered high enough to guarantee that the engaged items were adequate measures of the factors. The rate of Bartlett's test of sphericity is statistically significant (p-value <.000) fortifying the statistical correlation between the above-mentioned variables. Those measures show the appropriateness of data for the need for handling factor analysis and presented evidence of initial reliability.

5.2 Construct validity

Factor validity is revealed by analysing its indicators relationship with other factors, both associated (i.e., convergent validity) and unassociated (i.e., discriminant validity) (Pallant 2011). Hair et al. (2006) suggested that the evidence of convergent validity is confirmed If the indicators load strongly on their associated constructs (p>.50). In addition, the factors must be tested in order to discriminant validity, which could be achieved if the indicators are different from other unassociated indicators and load stronger on their associated factors than on any other factors. Items which have loadings under the

threshold must be dropped from the final instrument. Moreover, items loading on multiple factors must be dropped also. Nonetheless, Lewis, Templeton and Byrd (2005) recommended that subjective judgement must be applied, so that items with strongly justified theoretical relevance are not lost in the process. essential element analysis with Varimax rotation has been used to evaluate the validity of the instrument. The final instrument of 33 items representing 7 separate factors which have been tested in order to check the robustness of the measurement. The factor analysis showed a logical grouping with the identified constructs, ensuring the accuracy of the proposed constructs. All the 33 items have loadings on their related constructs over the cut-off of 0.50, thereby confirming convergent validity. Furthermore, all items load stronger on their associated construct than on other constructs, suggesting good discriminant validity. Thus, the outcomes show that factors can be applied to evaluate the conceptual research model and hypotheses.

5.3 Final reliability

According to Hair et al. (2006), Cronbach's alpha is commonly used to measure the reliability with a range from 0 (totally unreliable) to 1 (completely reliable). An alpha statistic of 0.60 to 0.70 is considered to be the lower limit of acceptability and sufficient for exploratory research, but 0.8 or higher is inevitably more desirable, and beyond .90 could pose a problem of multicollinearity(Nunnally & Bernstein 1967). The reliability test has been conducted during the pilot study data to evaluate the internal consistency of every group of items for each factor. The reliability function of the Statistical Package for the Social Sciences (SPSS) has been used to calculate Cronbach's alpha. The outcomes present that the reliability of the factors range from .79 to .93, which shows statistically significant results because they fall within the recommended rates. Consequently, factor reliabilities are considered to be sufficient.

6 CONCLUSION AND FUTURE WORK

This research seeks to study the challenges of cloud forensics and to highlight the relationship between Omani LEAs and Local CSPs. A wide range of existing research in CFR has a framework and prototype for solutions was quantified. However, as previous literature has shown, there is a knowledge gap in the relationship between the CSPs and LEAs in cloud forensics from a legal and technical perspective, the research highlights the importance of this relationship in order to achieve a high level of readiness, segregation of duties and responsibility.

To achieve the objectives, the researcher will use an interpretive qualitative case study approach, and the relationship between the CSPs and LEAs will be investigated. This research is expected to contribute to the body of knowledge of cloud forensics as the development of new theory, and a practical contribution is expected, where new insights and vision to decision and policymakers, CSPs and LEAs to improve this relationship.

7 REFERENCES

A Vouk, M 2008, 'Cloud computing–issues, research and implementations', *Journal of computing and information technology*, (16:4), pp. 235-46.

Ab Rahman, NH, Glisson, WB, Yang, Y & Choo, K-KR 2016, 'Forensic-by-design framework for cyber-physical cloud systems', *IEEE Cloud Computing*, (3:1), pp. 50-9.

Al-Gharibi, MW, Matthew; Yeoh, William 2018, 'Risks of Critical Infrastructure Adoption of Cloud Computing within Government', paper presented to 17th Australian Cyber Warfare Conference (CWAR), Melbourne.

Al-Gharibi, MW, Matthew; Yeoh, William 2019a, 'Government Cloud Computing Security Guidelines Similarities, Differences, and Gaps Related to Cyber Warfare', paper presented to 18th Australian Cyber Warfare Conference (CWAR), Melbourne.

Al-Gharibi, MW, Matthew; Yeoh, William 2019b, 'Risks of Critical Infrastructure Adoption of Cloud Computing by Government', *International Journal of Cyber Warfare and Terrorism (IJCWT)*.

Al-Kalbani, A 2017, 'A compliance based framework for information security in e-government in Oman'.

Al Husaini, YA-K, Haider; Warren, Matthew; Pan, Lei 2018a, 'A Model to Facilitate Collaborative Digital Forensic Investigations for Law Enforcement: The Royal Oman Police as a Case Study', paper presented to Cyber Forensic and Security Conference, Tonga.

Al Husaini, YW, Matthew; Pan, Lei 2018b, 'Cloud forensics relationship between the Law Enforcement and Cloud Service Providers', *17th Australian Cyber Warfare Conference (CWAR), Melbourne.*

Al Husaini, YW, Matthew; Pan, Lei 2018c, 'Cloud forensics relationship between the Law Enforcement and Cloud Service Providers', paper presented to 17th Australian Cyber Warfare Conference (CWAR), Melbourne.

Aladalah, M, Cheung, Y & Lee, VC 2016, 'Winning Digital Citizens: a Model and Instrument', in *PACIS*, p. 336.

Alenezi, A, Hussein, RK, Walters, RJ & Wills, GB 2017, 'A Framework for Cloud Forensic Readiness in Organizations', *2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, pp. 199-204.

Almulla, SA, Iraqi, Y & Jones, A 2014, 'A state-of-the-art review of cloud forensics', *Journal of Digital Forensics, Security and Law*, (9:4), pp. 7-28.

Alqahtany, S, Clarke, N, Furnell, S & Reich, C 2017, 'A forensic acquisition based upon a cluster analysis of non-volatile memory in IaaS', in *Anti-Cyber Crimes (ICACC), 2017 2nd International Conference on*, pp. 123-8.

Ballou, S 2010, *Electronic crime scene investigation: A guide for first responders*, Diane Publishing.

Brown, SR 1996, 'Q methodology and qualitative research', *Qualitative health research*, (6:4), pp. 561-7.

Cohen, J 1960, 'A coefficient of agreement for nominal scales', *Educational and psychological measurement*, (20:1), pp. 37-46.

De Marco, L 2015, 'Forensic Readiness Capability for Cloud Computing', Ph.D. thesis, 10187642 thesis, University College Dublin (Ireland).

Du, X, Le-Khac, N-A & Scanlon, M 2017, 'Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service', *arXiv preprint arXiv:1708.01730*.

Dykstra, J 2013, 'Seizing electronic evidence from cloud computing environments', *IGI Global*.

Elyas, M, Maynard, SB, Ahmad, A & Lonie, A 2014, 'Towards a systemic framework for digital forensic readiness', *Journal of Computer Information Systems*, (54:3), pp. 97-105.

Gartner 2018, *Gartner Forecasts Worldwide Public Cloud Revenue to Grow 21.4 Percent in 2018*, <https://www.gartner.com/newsroom/id/3871416>.

Grispos, G, Storer, T & Glisson, WB 2013, 'Calm before the storm: the challenges of cloud', *Emerging digital forensics applications for crime detection, prevention, and security*, vol. 4, no. 1, pp. 28-48.

Grobler, C, Louwrens, C & von Solms, SH 2010, 'A framework to guide the implementation of proactive digital forensics in organisations', in *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, pp. 677-82.

Hair, JF, Black, WC, Babin, BJ, Anderson, RE & Tatham, RL 2006, *Multivariate data analysis (Vol. 6)*, Upper Saddle River, NJ: Pearson Prentice Hall.

Harvey, RJ, Billings, RS & Nilan, KJ 1985, 'Confirmatory factor analysis of the Job Diagnostic Survey: Good news and bad news', *Journal of applied psychology*, (70:3), p. 461.

ISO 27037 2012, *IEC Information Technology-Security Techniques-Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*.

ISO/27043 2015, 'Information technology - Security techniques - Incident investigation principles and processes', *ISO/IEC*.

Kebande, VR & Venter, H 2016, 'Requirements for achieving digital forensic readiness in the cloud environment using an NMB solution', in *11th International Conference on Cyber Warfare and Security: ICCWS*, p. 399.

Kebande, VR & Venter, HS 2014, 'A cloud forensic readiness model using a Botnet as a Service', in *The International Conference on Digital Security and Forensics (DigitalSec2014)*, pp. 23-32.

Kohn, MD, Eloff, MM & Eloff, JH 2013, 'Integrated digital forensic process model', *Computers & Security*, vol. 38, pp. 103-15.

Landis, JR & Koch, GG 1977, 'The measurement of observer agreement for categorical data', *biometrics*, pp. 159-74.

Lewis, BR, Templeton, GF & Byrd, TA 2005, 'A methodology for construct development in MIS research', *European Journal of Information Systems*, (14:4), pp. 388-400.

Likert, R 1932, 'A technique for the measurement of attitudes', *Archives of psychology*.

Liveri, D & Skouloudi, C 2016, 'Exploring Cloud Incidents', *The European Network and Information Security Agency (ENISA)*, pp. 1-14.

MacKenzie, SB, Podsakoff, PM & Podsakoff, NP 2011, 'Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques', *MIS quarterly*, vol. 35, no. 2, pp. 293-334.

Makutsoane, MP & Leonard, A 2014, 'A conceptual framework to determine the digital forensic readiness of a Cloud Service Provider', in *Management of Engineering & Technology (PICMET), 2014 Portland International Conference on*, pp. 3313-21.

Mell, P & Grance, T 2011, 'The NIST definition of cloud computing'.

Mell, P & Grance, T 2014, 'Nist cloud computing forensic science challenges', *Draft Nistir*, vol. 8006.

Moore, GC & Benbasat, I 1991, 'Development of an instrument to measure the perceptions of adopting an information technology innovation', *Information systems research*, vol. 2, no. 3, pp. 192-222.

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 on*, pp. 162-7.

Nahm, AY, Rao, SS, Solis-Galvan, LE & Ragu-Nathan, T 2002, 'The Q-sort method: assessing reliability and construct validity of questionnaire items at a pre-testing stage', *Journal of Modern Applied Statistical Methods*, (1:1), p. 15.

Neuman, WL 2011, 'Social Research Methods: Qualitative and quantitative approaches (7th ed.).', *Boston, MA: Pearson Education, Inc.*

NIST 2014, 'Cloud Computing Forensic Science Challenges', no. Cloud Computing Forensic Science Challen.

Nunnally, J & Bernstein, I 1967, 'Berge JMt', *Psychometric theory: McGraw-Hill New York*.

Pallant, J 2011, 'Survival manual', *A step by step guide to data analysis using SPSS*.

Ras, D & Venter, H 2015, 'Proactive digital forensics in the cloud using virtual machines', in *Computing, Communication and Security (ICCCS), 2015 International Conference on*, pp. 1-6.

Reith, M, Carr, C & Gunsch, G 2002, 'An examination of digital forensic models', *International Journal of digital evidence*, (1:3), pp. 1-12.

Ruan, K & Carthy, J 2012, 'Cloud computing reference architecture and its forensic implications: A preliminary analysis', in *International Conference on Digital Forensics and Cyber Crime*, pp. 1-21.

Ruan, K, Carthy, J, Kechadi, T & Baggili, I 2013, 'Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results', *Digital Investigation*, (10:1), pp. 34-43.

Ruan, K, Carthy, J, Kechadi, T & Crosbie, M 2011, 'Cloud forensics', in *IFIP International Conference on Digital Forensics*, pp. 35-46.

Selamat, SR, Yusof, R & Sahib, S 2008, 'Mapping process of digital forensic investigation framework', *International Journal of Computer Science and Network Security*, (8:10), pp. 163-9.

Sibiya, G, Fogwill, T, Venter, HS & Ngobeni, S 2013, 'Digital forensic readiness in a cloud environment', in *AFRICON, 2013*, pp. 1-5.

Trenwith, PM & Venter, HS 2013, 'Digital forensic readiness in the cloud', in *Information Security for South Africa, 2013*, pp. 1-5.

Valjarevic, A & Venter, H 2013, 'A Harmonized Process Model for Digital Forensic Investigation Readiness', in *IFIP International Conference on Digital Forensics*, pp. 67-82.

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

Zhang, S, Wang, L & Han, X 2014, 'A KVM virtual machine memory forensics method based on VMCS', in *Computational Intelligence and Security (CIS), 2014 Tenth International Conference on*, pp. 657-61.

Zhao, Y & Duncan, B 2018, 'Could Block Chain Technology Help Resolve the Cloud Forensic Problem?', *CLOUD COMPUTING 2018*, p. 49.

Appendix 1 : List of measurement items

Construct	No	Survey Items	Reference
SOPs & Standards	SS1	Procedures, model or framework for cloud forensic investigations.	(Liveri & Skouloudi 2016; NIST 2014; Ruan et al. 2013)
	SS2	best practices for cloud forensic investigations	(Liveri & Skouloudi 2016; NIST 2014)
	SS3	A guideline on cooperation between CSPs and LEAs, in cases of an cloud forensics investigation.	(Liveri & Skouloudi 2016; NIST 2014; Ruan et al. 2013)
	SS4	An agreement on the recording of the chain of custody among all parties in an investigation.	(NIST 2014; Ruan et al. 2013)
	SS5	An agreement and guideline on preparing cloud forensic reports to ensure standard format.	(Liveri & Skouloudi 2016; Ruan et al. 2013)
Readiness	R1	Cloud forensic readiness with LEAs.	(Liveri & Skouloudi 2016)
	R2	Cloud forensic readiness with CSPs.	(Liveri & Skouloudi 2016)
	R3	Conducting plans and possible scenarios,	(Liveri & Skouloudi 2016; NIST 2014)
	R4	Test and verify tools (hardware and software) used in cloud forensics investigations.	(NIST 2014)
	R5	A policy in the CSPs to reinforce the proactive cloud forensics and ensure all procedures are performed in a standard fashion.	(Ruan et al. 2013)
	R6	Digital forensics staff in the LEAs provided with up-to-date training on cloud forensic knowledge.	(Liveri & Skouloudi 2016; NIST 2014)
Accountability	A1	Accountability of organisations actions and roles in cloud forensics investigations.	(Liveri & Skouloudi 2016; NIST 2014)
	A2	Accountability of individuals' actions and roles towards cloud forensics investigations.	(Liveri & Skouloudi 2016; NIST 2014)
	A3	The enforcement of cloud forensics investigations standards and procedures across the organization	(NIST 2014)
	A4	The appropriateness of specific sanctions in violating cloud forensics investigations standards	(Al-Kalbani 2017)
	A5	Severity of violation of the Cloud Forensics investigations (Legal damages, consequences, etc.)	(Al-Kalbani 2017)
Segregation of Duties	SD1	An agreement on the division of responsibilities	(Liveri & Skouloudi 2016; NIST 2014)
	SD2	Segregation of duties to avoid the conflict of interest and overlap between the functions of LEAs and CSPs.	(Liveri & Skouloudi 2016; NIST 2014)
	SD3	Understand ability and clarity of the cloud forensics investigations Standards and procedures	(NIST 2014)
	SD4	The clarity of employees' roles and responsibilities towards cloud forensics investigations	(Al-Kalbani 2017)
Laws & Regulations	LR1	Laws or regulations governing the work of cloud service providers CSP.	(Ruan et al. 2013)
	LR2	Laws or regulations cover aspects of Cloud Forensics investigations.	(Liveri & Skouloudi 2016; NIST 2014; Ruan et al. 2013)
	LR3	Service Level Agreement (SLA), should be covering the cloud forensics terms such as tools, supported technologies, and access granted regarding forensic investigation.	(Liveri & Skouloudi 2016; NIST 2014; Ruan et al. 2013)
	LR4	Encourage and participate in international conventions to facilitate access to an exchange of evidence during cloud forensics investigations with International level.	(Liveri & Skouloudi 2016; NIST 2014; Ruan et al. 2013)
	LR5	Consult the legal experts in CSPs or externally, in multi-jurisdiction/ multi-tenant cases in relation to forensic investigations.	(NIST 2014)
Trustworthiness	T1	The Team of the first responder at CSPs should be well trained and certified in cloud forensics on how to handle and maintain digital evidence?	(NIST 2014; Ruan et al. 2013)
	T2	Continuity of business and services are the top priorities for CSPs	(NIST 2014)
	T3	Functionality of digital forensics in satisfying the cloud forensics investigations requirements	(Al-Kalbani 2017; NIST 2014)
	T4	Users' confidence of maintain evidence integrity in CSPs	(Al-Kalbani 2017; NIST 2014)
Cloud forensics technology compatibility	TC1	The appropriateness of technical requirements for satisfying cloud forensic standards	(Al-Kalbani 2017; Ruan et al. 2013)
	TC2	Standardization of cloud forensic technologies	(Al-Kalbani 2017; NIST 2014)
	TC3	Interoperability of cloud forensic technologies with operational technologies	(Al-Kalbani 2017)
	TC4	Perceived impact in terms of technical burdens and cost	(Al-Kalbani 2017)