OIC-CERT Journal of Cyber Security
Volume 2, Issue 1 (February 2020)
19 – 29

Cloud Forensic Challenges and Recommendations: A Review

Warusia Yassin[1], Mohd Faizal Abdollah[2], Rabiah Ahmad[3], Zahri Yunos[4], and Aswami Ariffin[5]
[1,2,3]Centre for Advanced Computing Technology, Faculty of Information and Communications Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
[4,5]CyberSecurity Malaysia, Cyberjaya, Malaysia
[1]**s.m.warusia@utem.edu.my**

ARTICLE INFO

Article History
Received 22 May 2019
Received in revised form 15 Aug 2019
Accepted 25 Sep 2019

Keywords:
cloud computing, forensic investigation, challenges, recommendation, forensic phases

ABSTRACT

Cloud computing becomes more popular since the emergence of the Fourth Industrial Revolution (IR 4.0) as almost all internet services are highly dependent on high-end networks of server computers. The large-scale used on the internet around the world may cause the cloud server to be highly exposed to cyber threats and it is very difficult to apply forensic method specifically in conducting cloud forensic investigation. Subsequently, the lack of digital investigation may increase the threats towards cloud environment. Consequently, the cloud forensic investigation needs to be recognized for any incident happened in cloud services. Thus, this paper will review the the challenges in conducting a forensic investigation on cloud computing and the challenges are described according to cloud forensic investigation phase, which are identification, collection, examination and analysis, and lastly reporting and presentation. Moreover, recommendation to overcome current cloud forensic challenges which were specified by previous researches also being provided. This review will be beneficial to the community in order to overcome the challenges of cloud forensic investigation in the future.

I. INTRODUCTION

Cloud is a technology that is no longer new, and the technology has already been used for various services. The continuous increase in the volume and detail of data captured by establishments such as Internet of Things (IoT), has produced an overwhelming flow of data whether the data are in a structured or unstructured format. However, many customers remain reluctant to move their business IT infrastructure completely to a cloud environment. This is because security is one of the main concerns of customers and unknown threat need to be considered. The issues in security are also related to the ability to perform digital investigations in cloud sector [1]. With the rising acceptance of cloud computing, the attacker is starting to target cloud services and the incident will probably increase in the future. Furthermore, an attacker might leak confidential information from a victim by abusing a cloud storage service that allows users to store documents and images and access them through endpoint devices such as smartphone [2].

Cloud computing technology provides demanding usage of computing resources with minimal effort of management and cloud service provider interaction [3]. The cloud service uses virtualized resources that can be accessed by common users without running out of resources [4].

ISSN 2636-9680
eISSN 2682-9266

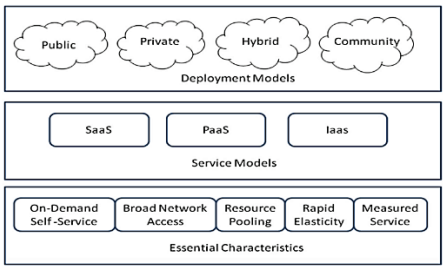

Fig.1: NIST Cloud Model [5]

The National Institute of Standards and Technology (NIST) defines cloud computing as a model with which to enable convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort [4].

There are several types of cloud that are currently provided by the cloud service provider. A cloud infrastructure that is owned by a cloud service provider is called a public cloud. The service provider is responsible to manage the cloud while distributing and selling the cloud resources to other companies [6]. In a private cloud, the cloud infrastructure is for the exclusive use of one company only. Thus, the company owns the cloud and uses the resources. Thus, the company, or a contracted company, is responsible for maintaining the cloud [6]. A cloud infrastructure that is owned and used by several companies can be called a community cloud. This type of cloud service is managed by the organization or a third party [6]. Most hybrid clouds combine public cloud with private cloud. Although the hybrid cloud uses multiple types of clouds, each of the modules still functions separately [6].

TABLE 1: Types of Cloud

Author	Public	Private	Hybrid	Community
(Sharma, 2016) [7]	/	/	/	
(Park et al., 2018) [8]	/	/	/	/
(Ho et al., 2018) [30]	/	/		
(Delport, 2013) [6]	/	/	/	/
(Birk and Wegener, 2011) [9]	/	/	/	/
(Doran, 2014) [10]	/	/	/	
(Galvan, 2013) [4]	/	/	/	/
(Alex and Kishore, 2017) [5]	/	/	/	/

TABLE 1 shows that most authors mentioning and describe types of clouds that has been made by the Cloud Service Provider based on the customer needs. This shows that most common types of cloud will and probably become a target of the attacker with malicious intent to steal the data from Cloud Service Provider.

There are three types of cloud computing service models which are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [6].

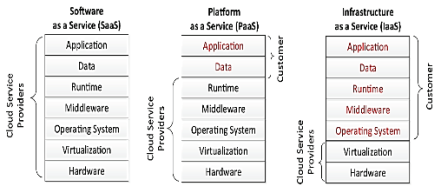

Fig. 2: Layers Architecture of Cloud Service [11]

In the Infrastructure as a Service (IaaS) model, the customer uses the virtual machine provided by the CSP for installing his own system on it. The system can be used like any other physical computer with a few limitations. However, the additive power over the system comes along with additional security obligations. Platform as a Service (PaaS) offerings provide the capability to deploy application packages created using the virtual development environment supported by the CSP. For the efficiency of Software Development Process this service model can be propellant. In the Software as a Service (SaaS) model, the customer makes use of a

service run by the CSP on a Cloud infrastructure. In most of the cases this service can be accessed through an API for a thin client interface such as a web browser.

II. CLOUD FORENSIC

Today, digital forensics has become more popular with law enforcement recognizes its function as to exploit criminal in cybercrime section. This also includes gathering the evidence, including digital devices such as smartphones, computer and smart sensors with can help police investigations. However, with the current tools that are sometimes not capable of analyzing the evidence because of compatibility issues, encryption or lack of training causing digital forensics to become inferior to be applied. Also, because of data management issues, most of the data evidence needs to be analyzed in a longer period of time that takes weeks to several months [12].

Although digital forensics has been established for several years, there is no specific or consistent methodology that can become a guide especially for cloud technology. With the increasing number of digital evidence that has been captured into laboratories, digital forensic methodology needs to be prioritized first in order to reduce the risk of evidence to be questioned during judicial proceedings [13,14].

Many authors have presented their understanding regarding cloud forensic by using the model, framework, layer or even process. However, all of these are included in the phases of cloud forensic investigation. Many authors have discussed about the phases and they are shown in **TABLE 2**.

TABLE 2: Number of Phases in Cloud Forensic

Author & Year	Research Title	Number of Phases
(Alex and Kishore, 2017) [5]	Forensics framework for cloud computing	4 Phases
(Martini and Choo, 2012) [14]	An integrated conceptual digital forensic framework for cloud computing, Digital Investigation	4 Phases
(Raju and Geethakumari, 2017) [15]	An advanced forensic readiness model for the cloud environment	4 phases
(Martini and Choo, 2013) [14]	Cloud storage forensics: OwnCloud as a case study	4 Phases
(Quick and Choo, 2013) [17]	Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?	5 Phases
(Shah and Malik, 2014) [18]	An approach towards digital forensic framework for cloud	4 Phases
(Rani and Geethakumari, 2015) [19]	An efficient approach to forensic investigation in cloud using VM snapshots	4 Phases
(Martini and Choo, 2012) [14]	An integrated conceptual digital forensic framework for cloud computing	4 Phases
(Quick and Choo, 2014b) [20]	Google drive: Forensic analysis of data remnants	4 Phases
(Pichan et al., 2015) [21]	Cloud forensics: Technical challenges, solutions and comparative analysis	6 Phases
(Easwaramoorthy et al., 2016) [22]	Digital forensic evidence collection of cloud storage data for investigation	4 Phases
(Khan et al., 2016) [23]	A Comprehensive Review on Adaptability of Network Forensics Frameworks for Mobile Cloud Computing A Comprehensive Review on Adaptability of Network Forensics Frameworks for Mobile Cloud Computing	4 Phases
(Ahmed Khan and Ullah, 2017) [24]	A log aggregation forensic analysis framework for cloud computing environments	5 Phases
(Almulla et al., 2014) [25]	a State-of-the-Art Review of Cloud	6 Phases

ISSN 2636-9680
eISSN 2682-9266

Author & Year	Research Title	Number of Phases
(Delport et al., 2011) [26]	Isolating a cloud instance for a digital forensic investigation	7 Phases
(Damshenas et al., 2012) [27]	Forensics investigation challenges in cloud computing environments	4 Phases
(Birk and Wegener, 2011) [9]	Technical Issues of Forensic Investigations in Cloud Computing Environments	3 Phases
(Simou et al., 2016) [28]	A survey on cloud forensics challenges and solutions	4 Phases
(Horsman, 2018) [29]	Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics	3 Phases
(Ho et al., 2018) [30]	Following the breadcrumbs: Timestamp pattern identification for cloud forensics	3 Phases
(Quick and Choo, 2014a) [20]	Impacts of increasing volume of digital forensic data: A survey and future research challenges	10 Phases
(Zhao, 2017) [31]	Study and Realization of Digital Forensics Key Technology Based on Cloud Computing	5 Phases

Based on the table above, there are different numbers of phases proposed by the authors. The cloud forensic investigation starts with three phases and one of them proposed until 10 phases. Basically, the main phases in cloud forensics are identification, collection, examination, analysis and reporting. The majority of the authors proposed four or five phases in cloud forensics. However, some authors have separated the tasks inside the main phase to become another different phase such as [13,20,26,25]. Following the majority of the authors, the main phases for cloud forensic might be four main phases and the analysis of the phases is shown in **TABLE 3**. **TABLE 3** shows a comparative analysis cloud forensic layers based on the previous authors in this field. Based on **TABLE 3** which is a comparative analysis on previous cloud forensic layers above, we analyze every phase to choose the best phase of cloud forensic investigation. In phase 1, identification has been used for almost every authors. Identification means to identify the scope of action before conducting any cloud forensic investigation that identifies the key players and custodians as well as the best sources of potential electronic evidence that need to be accessed for collection. In Phase 2, collection of data is the most preferred phase after identification phase. Collection means collecting digital information that may be relevant to the investigation.

TABLE 3: Comparative Analysis on Previous Cloud Forensic Layer

Author	Title	Phase 1	Phase 2	Phase 3	Phase 4
(Alex and Kishore, 2017) [5]	Forensics framework for cloud computing	Identification	Collection	Organization	Presentation
(Martini and Choo, 2012) [14]	An integrated conceptual digital forensic framework for cloud computing, Digital Investigation	Identification & Preservation	Collection	Examination & Analysis	Reporting & Presentation

Author	Title	Phase 1	Phase 2	Phase 3	Phase 4
(Raju and Geethakumari, 2017) [15]	An advanced forensic readiness model for the cloud environment	Identification	Collection	Examination	Analysis & Presentation
(Martini and Choo, 2013) [16]	Cloud storage forensics: ownCloud as a case study	Identification & Preservation	Collection	Examination & Analysis	Reporting & Presentation
(Shah and Malik, 2014) [18]	An approach towards digital forensic framework for cloud	Identification	Data Extraction, Preservation & Collection	Analysis/ Examination	Presentation
(Rani and Geethakumari, 2015) [19]	An efficient approach to forensic investigation in cloud using VM snapshots	Identification	Collection	Examination/ Analysis	Reporting/ Presentation
(Quick and Choo, 2014b) [20]	Google drive: Forensic analysis of data remnants	Prepare	Identify & Collect	Preserve (Forensic Copy)	Analysis
(Easwaramoorthy et al., 2016) [22]	Digital forensic evidence collection of cloud storage data for investigation	Identification & Preservation	Collection	Examination & Analysis	Reporting & Presentation
(Khan et al., 2016) [23]	A Comprehensive Review on Adaptability of Network Forensics Frameworks for Mobile Cloud Computing A Comprehensive Review on Adaptability of Network Forensics Frameworks for Mobile Cloud Computing	Collection	Examination	Analysis	Reporting
(Damshenas et al., 2012) [27]	Forensics investigation challenges in cloud	Identification	Collection	Preservation	Reconstruction

ISSN 2636-9680
eISSN 2682-9266

Author	Title	Phase 1	Phase 2	Phase 3	Phase 4
	computing environments				
(Simou et al., 2016) [28]	A survey on cloud forensics challenges and solutions	Identification	(Collection) Preservation	(Analysis) Examination	Presentation
(Rani and Sravani, 2016) [3]	Challenges of digital forensics in cloud computing environment	Identification	Collection & Preservation	Examination & Analysis	Reporting & Presentation

It involves removing the electronic device from the crime or incident scene and then imaging, copying or printing out the content. In Phase 3, examination and analysis are two different tasks, but can be combined in the same phase as the processes have similar objectives. This phase involves a systematic search of evidence related to the incident being investigated. The outputs of the examination are data objects found in the collected information; they may include system- and user-generated files. Analysis aims to draw conclusions based on the evidence found. Lastly, the fourth phase is reporting and presentation phase. The reports are based on proven techniques and methodology and the other competent forensic examiners should be able to duplicate and reproduce the same results. The results are then presented either in the court or not in the presence of a judge and juries. In conclusion, it can simplify that the major phases of cloud forensic investigation based on the majority of authors are identification, collection, examination and analysis, as well as reporting and presentation.

III. CHALLENGES IN CLOUD FORENSIC

Several challenges have been identified in the first phase of investigation. [3] described that it is difficult to access evidence in the logs when investigating in a cloud computing environment since it has several factors that need to be done. Consequently, [3] give a solution through accessing the logs in the eucalyptus cloud environment will ease the investigator to access logs in a cloud environment. With the lack of control in cloud system and lack of customer awareness, the investigator will face difficulties in identifying which cloud that has been affected. Thus, synchronization of volatile data and third-party member need to supply the logging information to cloud service provider and cloud user [3]. [32] also explained jurisdictional issues which are important for investigator before doing an investigation since it relates to who has the jurisdiction to investigate an international incident in cloud system.

The collection phase is one of the crucial parts of the cloud forensic investigation because data evidence that has been collected need to be secure from tampering or any external factor. [3] explained one of the challenges are data integrity which is important in order to maintain the chain of custody. [3] proposed a solution called Trust Platform Module (TPM) which preserves the integrity and confidentiality of the data in the cloud and using trained and qualified personnel will maintain chain of custody. [32] explained that investigator also has a minimum control and access to client side which is one of the possible data evidences that need to be collected. [32] also give a solution of using remote and control log server will shorten the process of digital

forensic investigation. [18] also said physical seizure is difficult to obtain for data collection since cloud does not have physical server. By using static data acquisition via virtual snapshot technique with fuzzy clustering method, it can be used for determining whether the VM is under safe or unsafe mode [18].

The third phase of cloud forensic investigation, which is an examination and analysis focusing on the analysis of the data evidence and what sort of tools that need to be considered as the investigation is going through. However, the lack of specific tools for cloud forensic [3] and lack of tested and certified tools [33] make the investigation is difficult to conduct. [3] proposed OWADE (Offline Windows Analysis and Data) which an open source software specifically for cloud forensic tools. Encase and FTK software are also available which are commercial digital forensic tools [3].

Finally, the last phase of cloud forensic investigation, which is reporting and presentation. [14] addressed the issues of metadata and logs can be modified to remove the traces of unauthorized access and malicious activities. This issue has been given a solution by [14] which stressed on the importance of keeping the data secure and does not break the chain.

Besides previous cloud forensic challenges and their solutions, **TABLE 4** shows challenges of cloud forensic based on category. It focuses on three phases, which are Identification, Collection, besides Examination and Analysis with the authors recommend to be the best method to encounter the problem in the cloud forensic investigation.

TABLE 4: Challenges of Cloud Forensic based on Category

Phase	Author	Challenges (Category)	Description	Recommendation
Identification	(Hay et al., 2011) [34]	Physical location	Unknown location	CSPs must ensure the flexibility and availability of the sources reserved
	(Alhamad et al., 2010) [35]	SLA issue	Lack of formal SLA terms	Must have forensic request in SLA from CSPs
	(Ruan and Carthy, 2013) [36]	System level logs	Lack of information on logs	Should contain all information such as access, created and deletion of system logs.
	(Sang, 2013) [37]	Decentralize log	Issue of hypervisor level logs in forensic process	Must have framework
	(Ruan and Carthy, 2013) (Alhamad et al., 2010) (Pichan et al., 2015) [36,35,21]	SLA issue	Lack of SLA focus on forensic requirement	Should have SLA that contain flexibility and server availability and accessibility of the resource in CSPs
		Data issue	Data duplication	Must have unique identification
			Data encryption	Must have guideline or process for cloud investigation and legal activity

ISSN 2636-9680
eISSN 2682-9266

Phase	Author	Challenges (Category)	Description	Recommendation
Collection	(Liu et al., 2010) [[38]	Lack of trust	Issue of hypervisor platform, virtual environment and cloud platform	Should have proposed mechanism between hypervisor platform, virtual environment and cloud platform
	(Delport et al., 2011) [6]	Cloud infrastructure isolation issue	Vendor control isolation process	Need a standard isolation process which accepted by forensic manor
		Lack of specialized cloud forensic issue	Lack of commercialize on specific tools	The tools which accepted by the jurisdiction
Examination and analysis	(Dykstra and Sherman, 2012) (Zawoad and Hasan, 2013) [39,40]	Logging issue	Log from cloud	Logging framework
			Evidence log resources	Proper resources of log
	(Pichan et al., 2015) [21]	No encrypted data facility	Current technology has no encrypted data facility	Password and key management infrastructure
		Issue of acquisition log	More focus on hardware integration and evidence finding	Correlations of evidence

IV. PREVIOUS RESEARCH RECOMMENDATIONS

Normally, digital forensics require investigators to do data acquisition, especially live acquisition by seizing physical hardware such as servers, computers or smart devices. However, in the cloud, acquiring the data by seizing equipment might be impossible as the data are diverse and classified across multiple regions and multiple countries with different service models. Hence, the investigator needs to require another permission if the case involves another country which makes acquisition highly challenging. [41] proposed an approach using VM snapshots in a cloud environment. It consists of Intrusion Detection System into VMM to monitor and detect malicious activity between VMs. The process of the approach is CSP stores snapshots of a VM whose activities are identified as malicious by an intrusion detection system. CSP is then require to provide log files of the suspected VM for investigator to acquire the evidence.

Suspected VM also needs to be isolated so other uninvolved instances does not interfere with digital investigation process. [26] proposed seven isolation technique which are Instance Relocation, Server Farming, Failover, Address Relocation, Sandboxing, Man in the Middle (MITM) and Let's Hope for the Best (LHFTB). When doing live forensics analysis, preventing the instance of tampering with evidence is the highest priority for investigators. Also, instances must be protected from the of the external factor such as power outage if the investigator choose to do dead analysis.

[39] addressed technical and trust issues in cloud that are constantly challenging to

tackle when acquiring evidence from the cloud service model, especially Infrastructure-as-a-Service (IaaS). It provides a model layer of trust in the cloud layer, presenting cloud forensic examination and analyzing the available method for investigators. Also, it describes forensic tools which are currently available and know how to use it in each cloud layer.

Various threats such as data hijacking, data loss or leakage are more common in cloud computing thus, decreasing the trust of potential customers to invest their business into cloud computing. [42] proposed a solution name TrustCloud which is a framework for accountability and trust in Cloud Computing. It classifies the main component into four which are security, privacy, accountability and audibility. TrustCloud consists of three components in abstraction layer which are system layer, data layer and workflow layer. These layers have each their own different role and set of sub-components for each context that simplifies the problem and makes accountability more achievable.

Service Level Agreement or SLA is an agreement between the CSP and the client that describe service terms such as policies, performance, availability, billing and other important items. The reason SLA is important because actions can be taken in instances such violation or breach of contract involving either side. [35] explained factors or elements that need to be considered when designing an SLA in cloud computing. The paper proposed a method to maintain the trust and reliability between each party involved during the negotiation process after investigating the negotiation strategies between CSP and client.

Additionally, [14] proposed an integrated conceptual digital forensic framework, emphasizing the differences in the preservation of forensic data and the collection of cloud computing data for forensic purposes. The framework is based on NIST framework and it is considered as one of the most widely used and accepted in forensic frameworks.

V. CONCLUSION

Cloud forensic has been recognized by the previous researchers. From cloud forensic layers or process to a solution and recommendation has been proposed, but they are not conclusive for investigators to use as a guide. With the comparative analysis, previous solution and possible types of evidence that can be found in cloud environments, this review can contribute to becoming a guide for investigators in cloud forensic investigation. The solutions and recommendations that have been proposed by the previous researchers are important contribution which can assist investigators to solve the issues in each phase of forensic investigation.

VI. REFERENCES

[1] S.K.A. Manoj and D.L. Bhaskari, "Cloud forensics-A framework for investigating cyber attacks in cloud environment," *Procedia Computer Science*, 85 (Cms), pp.149–154, 2016.

[2] H. Chung, J. Park, S. Lee, and C. Kang, "Digital forensic investigation of cloud storage services," *Digital Investigation*, 9 (2), pp.81–95, 2012.

[3] D.R. Rani, and P.L. Sravani, "Challenges of digital forensics in cloud computing environment," *Indian Journal of Science and Technology*, 9 (17), 2016.

[4] M. Galvan, Cloud Computing : Incident response and digital forensics, A Capstone Project Submitted to the Faculty of Utica College December 2013.

[5] M.E. Alex, and R. Kishore, "Forensics framework for cloud computing," *Computers and Electrical Engineering*, 60, pp.193–205, 2017,

[6] W. Delport, Forensic evidence isolation in clouds, submitted to the Faculty of Engineering, Built Environment and Information Technology University of Pretoria, November 2013.

[7] S. Sharma, "Expanded cloud plumes hiding Big Data ecosystem," *Future*

ISSN 2636-9680
eISSN 2682-9266

Generation Computer Systems, 59, pp.63–92, 2016.

[8] S. Park, Y. Kim, G. Park, O. Na, and H. Chang, "Research on digital forensic readiness design in a cloud computing-based smart work environment," *Sustainability (Switzerland)*, 10 (4), pp.1–24, 2018.

[9] D. Birk, and C. Wegener, "Technical issues of forensic investigations in cloud computing environments," in *2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, Oakland, CA, USA, 2011, pp.1–10,

[10] M.D. Doran, A forensic look at Bitcoin cryptocurrency, A Capstone Project Submitted to the Faculty of Utica College, in Partial Fulfillment of the Requirements for the Degree of Master of Science in Cybersecurity, 2014.

[11] V. Roussev, I. Ahmed, A. Barreto, S. McCulley, and V. Shanmughan, "Cloud forensics–Tool development studies & future outlook," *Digital Investigation*, Vol. 18, pp.79–95, 2016.

[12] S.L. Garfinkel, "Digital forensics research : The next 10 years", *Digital Investigation*, Vol 7, 2010, pp. 64-73.

[13] D. Quick, and K.K.R. Choo, "Google drive: Forensic analysis of data remnants," *Journal of Network and Computer Applications*, Vol. 40, pp.179–193, 2014a.

[14] B. Martini, and K.K.R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digital Investigation*, 9 (2), pp.71–80, 2012,

[15] B.K.S.P.K. Raju and G. Geethakumari, "An advanced forensic readines. model for the cloud environment," in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, pp.765–771, 2017

[16] B. Martini and K.K.R. Choo, "Cloud storage forensics: OwnCloud as a case study," *Digital Investigation*, 10 (4), pp.287–299, 2013.

[17] D. Quick and K.K.R. Choo, "Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?," *Digital Investigation*, 10 (3), pp.266–277, 2013.

[18] J.J. Shah, and L.G. Malik, "An approach towards digital forensic framework for cloud," in *2014 IEEE International Advance Computing Conference (IACC)*, 2014, pp.798–801.

[19] D.R. Rani and G. Geethakumari, "An efficient approach to forensic investigation in cloud using VM snapshots.\," in *2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015*, 00 (c), 2015.

[20] D. Quick and K.K.R. Choo, "Impacts of increasing volume of digital forensic data: A survey and future research challenges," *Digital Investigation*, Vol. 11, Issue 4, pp.273–294, 2014b.

[21] A. Pichan, M. Lazarescu, and S.T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," *Digital Investigation*, 13, 2015, pp.38–57.

[22] S. Easwaramoorthy, S. Thamburasa, G. Samy, S.B. Bhushan and K. Aravind, "Digital forensic evidence collection of cloud storage data for investigation," in *2016 International Conference on Recent Trends in Information Technology, ICRTIT 2016*.,2016.

[23] S. Khan, M. Shiraz, A. W Abdul Wahab, A. Gani, Q. Han, Z. Abdul Rahman, "A comprehensive review on adaptability of network forensics frameworks for mobile cloud computing, *The Scientific World Journal*, 2014

[24] M.N. Ahmed Khan and S.W. Ullah, "A log aggregation forensic analysis framework for cloud computing environments," *Computer Fraud and Security*, Issue 7, July 2017, pp.11–16.

[25] S. Almulla, Y. Iraqi and A. Jones, "A State-of-the-art review of cloud," Journal of Digital Forensics, Security and Law (February 2015). 2014.

[26] W. Delport, M.S. Oliver and M.D. Kohn, "Isolating a cloud instance for a digital forensic investigation," in *Information Security for South Africa (ISSA2011) Conference*, (September), 2011, pp.145–153,

[27] M. Damshenas, A. Dehghantanha, R. Mahmoud and S. Bin Shamsuddin, "Forensics investigation challenges in cloud computing environments", in

Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012, 2012, pp.190–194.

[28] S. Simou, C. Kalloniatis, S. Gritzalis, and H. Mouratidis, "A survey on cloud forensics challenges and solutions," *Security and Communication Networks*, 9 (18), pp.6285–6314, 2016.

[29] G. Horsman, "Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics," *Computers and Security*, 73, pp.294–306, 2018.

[30] S.M. Ho, D. Kao and W.Y. Wu, "Following the breadcrumbs: Timestamp pattern identification for cloud forensics," *Digital Investigation*, 24, pp.79–94, 2018.

[31] B. Zhao, "Study and Realization of Digital Forensics Key Technology Based on Cloud Computing," Revista de la Facultad de Ingenieria, 32, pp.53–57, 2017.

[32] P.M. Trenwith, Digital Forensic Readiness in the Cloud, 2013.

[33] G. Grispos, T. Storer and W.B. Glisson, "Calm before the storm: the challenges of cloud computing in digital forensics," *International Journal of Digital Crime and Forensics*, 4 (2), pp.28–48, 2012.

[34] B. Hay, K. Nance and M. Bishop, "Storm clouds rising: Security challenges for IaaS cloud computing," *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2011, pp.1–7.

[35] M. Alhamad, T. Dillon, and E. Chang, "Conceptual SLA framework for cloud computing," in *4th IEEE International Conference on Digital Ecosystems and Technologies - Conference Proceedings of IEEE-DEST 2010, DEST 2010*, 2010 , pp.606–610.

[36] K. Ruan and J. Carthy, Cloud Computing Reference Architecture and Its Forensic Implications: A Preliminary Analysis, pp.1–21, 2013

[37] T. Sang, "A log-based approach to make digital forensics easier on cloud computing, " in *Proceedings of the 2013 3rd International Conference on Intelligent System Design and Engineering Applications, ISDEA 2013*, 2013, pp.91–94.

[38] D. Liu, J. Lee, J. Jang, and J. Zic, "A cloud architecture of virtual trusted platform modules", *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, Hong Kong, 2010, pp. 804-811.

[39] J. Dykstra and A.T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques," *Digital Investigation*, 9 (SUPPL.), pp.S90–S98, 2012.

[40] S. Zawoad and R. Hasan, Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems, 2013.

[41] R. Poisel, E. Malzer, and S. Tjoa, Evidence and cloud computing : The virtual machine introspection approach. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 4 (1), pp.135–152, 2012.

[42] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang and B.S. Lee, "TrustCloud: A framework for accountability and trust in cloud computing," *Proceedings - 2011 IEEE World Congress on Services, SERVICES 2011*, 2011, pp.584–588.

ISSN 2636-9680
eISSN 2682-9266

ISSN 2636-9680
eISSN 2682-9266