International Journal on Emerging Technologies **11**(5): 98-105(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

A Review of Cloud Forensic Investigation: Challenges, Recommendation and Readiness

W. Yassin[1], M.R. Baharon[1], N. Bahaman[1], Z.A. Abas[2] and M.F. Abdollah[2]

[1]Senior Lecturer, Centre for Advanced Computing Technology, Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia.

[2]Associate Professor, Centre for Advanced Computing Technology, Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia.

(Corresponding author: W. Yassin)

(Received 06 June 2020, Revised 09 July 2020, Accepted 24 July 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: The adoption of cloud computing technology globally getting extensive demanding as the resources could share comprehensively. Nevertheless, due to the large-scale utilization and dependency on high-end networks as well as servers, this technology also effected by cybercrime activity. The fact that cloud forensic investigation against these innovative and establishment of ultramodern computing technology, facing major challenges is undeniable, even though digital forensic methods been practiced and applied since few decades ago. For instance, acquisition of data become more difficult as the physical server geographically distributed, lack of information on logs to be investigate as the provider control the entire cloud platform, lack of forensic tools to analyse the evidence and many more. Hence, there is necessary to foreground literature study and comparative analysis more specifically in cloud forensic which involves a process of data collection, integrity of evidence, format complication and so forth. This paper present literature study which comprises a collection of analysis from several previous work that concern more on cloud forensic challenges, investigation and recommendation. Throughout the study, consequently, the readiness of cloud forensic been formed and described thoroughly to contribute an understanding of cloud forensic needs and as a reference's sources for research community. Beside this, it is also helping an industry to be in line with current trending particularly in cloud forensic.

Keywords: Cloud Computing, Cloud Forensic Investigation, Cloud Forensic Challenges, Cloud Forensic Readiness and Cybercrime.

I. CLOUD COMPUTING

Cloud computing growing rapidly due to the acceptance of this technology which applied in various services and field by surrounding community nowadays. Moreover, a lot of customers remain reluctant to move their IT infrastructure completely into cloud environment as its promises in term of cost saving, availability of services 24/7, flexible and so forth [1]. Specifically, cloud computing technology enables convenient, on-demand usage of computing resources with minimal management effort and service provider interaction [2]. It can be defined as applications and services that run on a distributed system using virtualized resources and accessed by common Internet protocols, networking standards and resources are virtual and limitless, and that details of the physical systems on which software runs are abstracted from the user [3]. 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 (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort [3].

These technologies available into different form of types such as public, private, hybrid and community [4] that has been developed by the cloud service provider based on the customers' needs. These types of cloud available in different service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [4]. An Infrastructure as a Service (IaaS) is a model where customer using 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 the capability to deploy application packages which 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.

The advantages of cloud computing include virtualized resources, parallel processing, security, and data service integration with scalable data storage. Cloud computing can not only minimize the cost and restriction for automation and computerization by individuals and enterprises but can also provide reduced infrastructure maintenance cost, efficient management, and user access. Cloud computing eliminates the costs and complexity of buying, configuring, and managing the hardware and software [1]. Cloud computing is heavily dependent on the Internet, and physical system, software, and data are stored on offsite servers. Therefore, having access to business resources via a Web browser makes it convenient for business owners, employees, and stakeholders to run a business. Unfortunately, although the cloud technology is widely

applied today, an open challenge concerning security aspect still need to be considered. The incident against cloud probably be increasing in the future as there is rising in the adoption of such technology comprehensively which can influence the attacker abusing storing services and leak the victimized confidential information [5]. Consequently, this issues also leads to the limitation of performing digital investigation in cloud sector [1].

II. CLOUD FORENSIC

Cloud computing growing rapidly due to the acceptance of this technology which applied in various services and field by surrounding community nowadays. Moreover, a lot of customers remain reluctant to move their IT infrastructure completely into cloud environment as its promises in term of cost saving, availability of services 24/7, flexible and so forth [1]. Currently, these services vulnerable to cyber-attacks and directly causing the need for digital forensic necessarily important and mandatory. Digital forensics has become prevalent because law enforcement recognizes that modern day life includes a variety of digital devices that can be exploited for criminal activity, not just computer system. However, organizations encounter that digital data comprises in cloud technology cannot be analyzed with today's tools because of format incompatibilities, encryption, or simply a lack of training. Otherwise, if the data can be analyzed, have to wait weeks or months of review process because of data management issues [6]. Unfortunately, there is no standard or consistent digital forensic methodology against cloud technology, but rather than a set of procedures and tools built from the experiences of law enforcement, system administrators, and hackers. The increase in the number and volume of digital devices seized and lodged with digital forensic laboratories for analysis also has been an issue raised over many years [7]. Thus, to reduce the risk of digital (forensic) evidence being called into question in judicial proceedings, it is important to have a rigorous methodology and set of procedures for conducting forensic investigations and examinations. The development of digital forensics methodologies needs to be built on these sound scientific principles [8]. The need for digital forensic analysis of cloud computing environment and applications has become customary [9]. Furthermore, CSPs must able to perform their own network forensics and identify legal evidence [10] if required.

III. CLOUD FORENSIC PHASES

Conventional digital forensic engaged with acquiring required information from the seized media which collected from the crime scene location. This is due to exercise of preservation procedure of that information, and subsequently deals with procedure of validation, analysis, interpretation, documentation, and presentation of collected and controlled evidence in facilitating law enforcement.

In contrast, in cloud cases, the required information may possibly in any place all over the globe, even away from related country boundaries. This could be a most challenging task to fully control the evidence for the purpose of collection, preservation, and validation. Nevertheless, in order to tackle this limitation, in recent years, various researchers have presented their idea and knowledge regards to cloud forensic phases (a.k.a. model, framework, layers or even process). Moreover, most of them comprehensively concern to highlights their recommendations or opinions about phases for cloud forensic investigation. Many authors had discussed about four major phases i.e. identification, collection, examination, and analysis as well as reporting for almost a decade as illustrated in Table 1.

Following majority of above authors, the main phases for cloud forensic defined to be four main phases. Based on this suggestion, a comparative analysis on cloud forensic layers which more focuses in 4 layers is presented in Table 2. Based on our comparative analysis, majority author has focused their intention only on phases of Identification, Collection, Examination and Analysis, and Reporting and Presentation and furthermore claimed these is the best phases practices for cloud forensic investigation.

For example, in an initial phase (Phase 1), an identification has been considered dominantly for almost by entire authors. An identification is a procedure of identifying the scope of action before conducting any cloud forensic investigation that identify the key players and custodians as well as best sources of potential electronic evidence which will need to be accessed for collection.

The collection of related information for forensic analysis is mandatory, as such, the collection phases (Phase 2) is considered by various author subsequently. Moreover, these phases generally involve action of collecting digital information that may be relevant to the investigation. For example, removing the electronic device from the crime or incident scene and then imaging, copying, or printing out the content. Thereafter, examination and analysis (Phase 3) phases been considered whereby both leads to a distinct task but the processes inside these phases shares common similar objective i.e. involving a process of systematic search of evidence that related to the incident being investigated.

Table 1: Number of Phases in Cloud Forensic.

Author & Year	Number of Phases
[11] Damshenas *et al.*, 2012	4 Phases
[8] Martini and Choo, 2012	4 Phases
[12] Martini and Choo, 2013	4 Phases
[13] Shah and Malik, 2014	4 Phases
[14] Quick and Choo, 2014b	4 Phases
[9] Rani and Geethakumari, 2015	4 Phases
[15] Easwaramoorthy et al., 2016	4 Phases
[10] Khan *et al.,* 2016	4 Phases
[16] Simou *et al.,* 2016	4 Phases
[17] Alex and Kishore, 2017	4 Phases
[18] Raju and Geethakumari, 2017	4 phases

Table 2: Comparative Analysis on Previous Cloud Forensic Layer.

Author	Phase 1	Phase 2	Phase 3	Phase 4
[8] Martini and Choo, 2012	Identification & Preservation	Collection	Examination & Analysis	Reporting & Presentation
[13] Shah and Malik, 2014	Identification	Data Extraction, Preservation & Collection	Analysis/Examination	Presentation
[9] Rani and Geethakumari, 2015	Identification	Collection	Examination/Analysis	Reporting/Presentation
[14] Quick and Choo, 2014b	Prepare	Identify & Collect	Preserve (Forensic Copy)	Analysis
[15] Easwaramoorthy et al., 2016	Identification & Preservation	Collection	Examination & Analysis	Reporting & Presentation
[10] Khan *et al.,* 2016	Collection	Examination	Analysis	Reporting
[16] Simou *et al.,* 2016	Identification	(Collection)Preservation	(Analysis)Examination	Presentation
[2] Rani and Sravani, 2016	Identification	Collection & Preservation	Examination & Analysis	Reporting & Presentation
[17] Alex and Kishore, 2017	Identification	Collection	Organization	Presentation
[9] Raju and Geethakumari, 2017	Identification	Collection	Examination	Analysis & Presentation

The output of examination is normally about data objects found in the collected information while analysis aims to draw conclusions based on the evidence found. Finally, the last phases that been suggested are reporting and presentation (Phase 4). The reports are based on proven techniques and methodology as well as the other competent forensic examiners should be able to duplicate and reproduce the same results. The results are then presented (a.k.a. presentation) either in the court or with the presence of judge and juries.

Hence, these major phases such as identification, collection, examination, and analysis, and reporting and presentation of cloud forensic investigation are recommended by majority authors.

IV. CHALLENGES AND RECOMMENDATION IN CLOUD FORENSIC

A number of researchers has highlighted the existing challenges in cloud forensic that facing by the community and nevertheless provide a recommendation to overcome issues related to cloud forensic investigations. After review and analyzing previous works from several authors, each existing challenges and available solution has been identified and emphasized accordingly into different phases of forensic investigation as presented in Table 3. Generally, digital forensics requires investigators to acquire the data lively by seizing physical hardware such as servers, computers, or smart devices.

Table 3: Challenges of Cloud Forensic based on Specific Category.

Phase	Author	Challenges (Category)	Description	Recommendation
Identification	[20] Hay *et al.,* 2011	Physical location	Unknown location	CSPs must ensure the flexibility and availability of the sources reserved
	[30] Alhamad *et al.*, 2010	SLA issue	Lack of formal SLA terms	Must have forensic request in SLA from CSPs
	[21] Ruan and Carthy, 2013	System level logs	Lack of information on logs	Should contain all information such as access, created and deletion of system logs.
	[22] Sang, 2013	Decentralize log	Issue of hypervisor level logs in forensic process	Must have framework
	[21] Ruan and Carthy, 2013 [30] Alhamad et al., 2010 [23] Pichan *et al.*, 2015	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
Collection	[24] Liu *et al.*, 2010	Lack of trust	Issue of hypervisor platform, virtual environment and cloud platform	Should have proposed mechanism between hypervisor platform, virtual environment and cloud platform

	[25] Delport *et al.,* 2011	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
	[16] Simou *et al.*, 2014	Maintaining chain of custody	Very hard to be maintain and required specific skills	Trained and qualified personnel
	[13] Shah and Malik, 2014	Physical seizure is difficult for data collection in cloud.	Data stored in virtual environment	Static data acquisition via Virtual snapshot technique
Examination and analysis	[26] Dykstra and Sherman, 2012 [27] Zawoad and Hasan, 2013	Logging issue	Log from cloud	Logging framework
			Evidence log resources	Proper resources of log
	[23] Pichan *et al.,* 2015	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
	[2] Rani and Sravani, 2016 [13] Shah and Malik, 2014	Forensic tools availability issues	Lack of tested and certified tools	Encase and FTK are commercial digital forensics tools
Reporting & Presentation	[8] Martini and Choo, 2012	Integrity of metadata	Metadata and access logs can be modified to remove traces of unauthorized access and other malicious activity	Metadata and other forms of audit data must be properly kept

However, in cloud, acquiring the data by seizing equipment might be a challenging or even impossible task as the data are diverse and classified ranging into multiple regions across country with different service models. Hence, investigator need to require another permission regarding involving procedure across country which makes acquisition highly challenging. In addition, preventing the instance from tampering with evidence is the highest priority for investigator when performing live forensic analysis and the entire instances must be protected from an external factor such as power outage incase the investigator choose to conduct dead analysis. This scenario difficult to predict as the cloud facility usually control by CSP entirely. Despite that, a number of researchers proposed several recommendations and come with their effective solution to overcome cloud forensic issues. For example, [28] proposed an approach using VM snapshots in cloud environment whereas it consists of Intrusion Detection System into VMM to monitor and detect malicious activity between VMs. The process of this approach is CSP stores snapshots of a VM, those activities are identified as malicious by an intrusion detection system and subsequently the CSP require to provide log files of the suspected VM for investigator to acquire the evidence. Furthermore, suspected VMs also need to be isolated due to the fact that other uninvolved instances do not interfere digital investigation process. Therefore, [25] proposed seven isolation technique such as Instance Relocation, Server Farming, Failover, Address Relocation, Sandboxing, Man in the Middle (MITM) and Let's Hope for the Best (LHFTB). Conversely, [26] addressed technical and trust issues in cloud which constantly turn to be challenging when acquiring evidence from the cloud service model especially Infrastructure-as-a-Service (IaaS). Henceforth, the author provides a model layer of trust in cloud layer, presenting cloud forensic examination and analyzing the available method for an investigator. Besides, the author also manages to describe forensic tools which are currently available and how to use it in each cloud layer. Lately, there is various threats such as data hijacking, data loss or leakage that much more effected the cloud computing and as a consequence this has cause decreasing of trust of potential customer to investing their business into cloud computing. Trust issues will cause huge impact particularly when the customer hard to accept the finding of forensic investigation as an evidence. For this reason, [29] proposed a solution namely TrustCloud which is a framework to solve issues of accountability and trust in Cloud Computing. This framework classifies the main component into four such as security, privacy, accountability, and audibility. TrustCloud consists of three components in abstraction layer which are system, data, and workflow whereas each these layers have 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 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 such violation or acting of breaching contract involve in either sides. [30] explained factors or elements that need to be considered when designing SLA in cloud computing. The paper proposed a method to maintain the trust and reliability between each party involved during negotiation process after investigating the negotiation strategies between CSP and client. Additionally, [8] 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 McKemmiexplosh and NIST framework consider it was two of the most widely used and accepted forensic frameworks.

V. CLOUD FORENSIC READINESS

The basis of forensic readiness is more concern on planning and designing a system for collecting and correlating the data using evidence from the risk profiling activities [31]. Moreover, the readiness phase is highly needed to assure that operations and infrastructure are competent to entirely support an investigation [16]. We addressed cloud forensic readiness into three factor i.e. technical, legal and organizational as summarized in Table 4.

The technical factors usually relate to technological aspects that influence forensic readiness in cloud environments. Cloud architecture, forensic technologies and cloud security are three major elements that can be take into account in measuring the readiness of cloud forensic. Cloud architecture is a system architecture that formulate in a specific way in order to increase forensics capabilities, which results in the acquiring of acceptable digital evidence. Besides, forensic technologies are referring to availability of forensic software or tools that are essential in a process of collecting evidence in any digital investigation.

These technologies must be reliable enough and more accurate in providing admissible evidence as absences of such procedures could causes difficulty in conducting a digital investigation. Due to the fact that in an effort to conduct a digital investigation, an incident be required to detectable by monitoring as this is a source of evidences. Henceforth, security programs in which can be referred as cloud security is mandatory in the digital forensic field. An example of widely applied technologies is an intrusion detection system, intrusion prevention systems, firewall, antivirus, anti-spyware and so forth. Usually, these are the factors are mean to support cloud forensic investigation in every single investigation processes.

Legal factors include an aspect that associated with an agreement between clients and cloud providers, multi-jurisdictions, and regulatory authorities. These factors can be grouped into three principle elements such as Service Level Agreement (SLA), regulatory and jurisdiction. Service Level Agreement (SLA) is a contract between a cloud service provider (CSPs) and customers whereas this document usually contain information on an offering services, including forensics investigations. As this is an official agreement, the SLA must precisely define CSP and customers' obligations affiliated with forensic investigations. Regulatory is a compliance to laws and regulations, such as acceptability of digital evidence in court and the chain of custody. There is a possibility where CSPs may provide cloud services from some other region, thus it is essential for an organization to determine the judicial regions if required and consider the entire multi-jurisdictions. These factors are crucial as an investigator need to consider a region of investigation in prior to investigating process. Each phase needs to have regulatory for all evidence and result analysis need to be preserve and chain of custody cannot be break until it will be presenting at the court.

Besides technical and legal factors, the other factor that must be considered is organizational and a number of previous researchers been focused on this factor. The organizational factors comprise the characteristics of an organization and its employees that can ease cloud forensic readiness. Strategy, training, and procedures are there major elements that can be considered in this factor. Readiness strategy is an organization's initiative to accomplish forensics readiness whereas these strategies pertains to how the readiness would work. This includes identifying hypothetical scenarios, possible evidence sources, and budget planning. In addition, training can be viewed as the arrangements of training series to technical staff and awareness series to nontechnical staff on forensics finest practices. A number of guidelines and instruction construct via the third element namely procedures i.e. proactive and reactive forensic procedures, in order to guide the digital forensics investigations. A company or specifically Cloud Service Provider (CSPs) must have and practice these elements with the aim to facilitate an investigator to perform investigation process more precisely. However, training internal staff is currently having an issue which it lacks realistic training data.

The entire above-mentioned factors and elements for each cloud forensic investigation phases summarized and has presented in Fig. 1. Based on this figure, the cloud forensic readiness divided into three major factors i.e. technical, legal and organization which influence by four principle cloud forensic phases i.e. identification, collection, examination, and analysis as well as reporting and presentation.

Usually, the forensic phases for architectural and security elements under the technical factors, only involve up to examination and analysis phases as it is more concern on availability (in term of readiness) of system architecture and security programs to perform forensic investigation. Besides, today available technology i.e. IDS, IPS, Firewall and any other monitoring tools are sufficient to support the entire phases of cloud forensic investigation. Furthermore, consideration for SLA and jurisdiction is possible during the phase of identification and collection in facilitate the investigation process while the process of regulatory possible to remain for all phases. Similarly, as SLA and jurisdiction, organization efforts in achieving cloud forensic investigation readiness is also can be practiced as highlighted by few researchers. In addition, the practice to conduct investigation process throughout procedures by investigators is also available nowadays as recommended by most of third-party providers. Hence, conducting forensic investigation towards cloud environment is possible as recommended by various researcher and the major phases that could be consider is identification, collection, examination, and analysis as well as reporting and presentation.

Table 4: List of Readiness Factors.

Factor	Phases												Author
	Identification			Collection			Examination/Analysis			Reporting/Presentation			
	Architecture	Technologies	Security	Architecture	Technologies	Security	Architecture	Technologies	Security	Architecture	Technologies	Security	
Technical Readiness Factors					•			•					[6] Garfinkel, 2010
				•									[8] Martini and Choo, 2012
				•	•								[4] Delport, 2013
	•	•	•	•	•	•	•	•	•				[13] Shah and Malik, 2014
	•				•			•					[32] Almulla *et al.*, 2014
					•	•							[33] Morioka and Sharbaf, 2015
	•	•			•	•		•			•		[19] Khan *et al.*, 2016
	•				•			•					[17] Alex and Kishore, 2017
	SLA	Regulatory	Jurisdiction	SLA	Regulatory	Jurisdiction	SLA	Regulatory	Jurisdiction	SLA	Regulatory	Jurisdiction	Author
Legal Readiness Factors	•		•	•		•							[25] Delport, 2013
		•	•	•	•	•		•			•		[8] Martini and Choo, 2012
	•					•							[32] Almulla *et al.*, 2014
	•		•	•		•							[16] Simou *et al.*, 2016
		•											[21] Ruan and Carthy, 2013
	•					•							[33] Morioka and Sharbaf, 2015
	Strategy	Training	Procedure	Strategy	Training	Procedure	Strategy	Training	Procedure	Strategy	Training	Procedure	Author
Organizational Readiness Factor	•												[19] Khan *et al.*, 2016
			•			•			•			•	[16] Simou *et al.*, 2016
		•	•										[33] Morioka and Sharbaf, 2015
	•	•		•	•								[6] Garfinkel, 2010

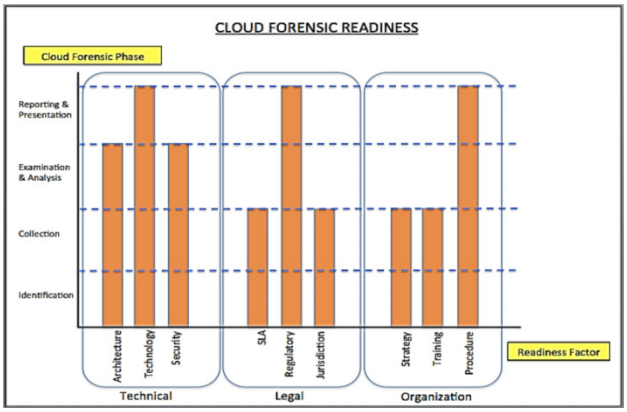

Fig. 1. Cloud Forensic Readiness.

Several authors have reviewed the challenges in performing forensic processes against cloud technology recently. Such challenges usually comprise the limitation on technical issues, readiness of related tools, current available solutions, comparative analysis, legal enforcement and many more. For example, in [34] the author highlighted the technical challenges in cloud forensic i.e. admission to logs accessibility and the available cloud forensic tools. Furthermore, in [35] the author manages to conduct a comparative analysis to provide awareness on the challenges more specific in the cloud forensic evidence collection. According to the author, the live forensic procedure is only can be performed in private cloud instead of public. Moreover, recently an author in [36] has conducted a systematic literature survey and claimed that there are huge challenges for each phase of cloud forensic i.e. identification, collection, examination, and reporting. Therefore, the need to be aware of the trends and constraints of forensic methods on cloud technology is essential. In addition, mechanisms such as studies or related reviews are needed as a reference for the relevant parties for the future. As the use of forensic methods on the cloud becomes increasingly complex and requires more serious attention, this work will help in terms of identifying the lack of forensic phases and application of such approach against today's technology.

VI. CONCLUSION

A number of existing literatures has highlighted the challenges of cloud forensic and the needs of forensic investigation against cloud facility. In addition, there are several researchers who have expressed their opinions on the most prevalent and currently used forensic phases which can be adopt into cloud forensic investigations. However, an effort to recommend standard phases which can be practiced by organization are limited. Furthermore, the availability or readiness of forensic investigation towards cloud environment is not well addressed by most researchers.In this paper, unlike previous literature, a number of previous works been studied systematically, analyzed and summarized.A standard cloud forensic phases identified and recommended based on existing challenges and available solution in cloud forensic investigation process. In order to facilitate forensic investigator in conducting their investigation and understanding of an organization on cloud forensic readiness, three different major factors i.e. technical, legal and organization as a standard reference considered and highlighted. These major factors have been divided into few elements which influence the cloud forensic readiness adoption such as architecture, technology, security, SLA, regulatory, jurisdiction, strategy, training and procedures. Hence, the entire provided information in this paper could be ease in the understanding and important of cloud forensic investigation specifically to research community.

VII. FUTURE SCOPE

Future scope will focus in forensic challenges on the technology which adopting cloud computing as a backend platform such as IoT.

ACKNOWLEDGEMENTS

The authors would like to express the appreciation to Inforsnet Group Research of Universiti Teknikal Malaysia Melaka (UTeM) in encouraging the authors to publish this paper. This work was supported by UTeM under the short grant PJP/2019/FTMK(5B)/S01676.

Conflict of Interest. The author declares no conflict of interest.

REFERENCES

[1]. S. K. A. Manoj and D. L. Bhaskari (2016). Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment. *Procedia Comput. Sci., 85*, 149–154.

[2]. D. R. Rani and P. L. Sravani (2106). Challenges of Digital Forensics in Cloud Computing Environment. *Indian J. Sci. Technol., 9*(17).

[3]. N. A. Le-Khac and K. K. R. Choo, Eds. (2020). Cyber and Digital Forensic Investigations, *74*. Cham: Springer International Publishing.

[4]. Delport, W. (2014). Forensic evidence isolation in clouds.

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

[6]. S. L. Garfinkel, (2010). Digital forensics research: The next 10 years. *Digit. Investig., 7*, pp. S64–S73.

[7]. D. Quick and K. K. R. Choo (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digit. Investig., 11*(4), 273–294.

[8]. B. Martini and K. K. R. Choo (2012). An integrated conceptual digital forensic framework for cloud computing. *Digit. Investig.*, *9*(2), 71–80.

[9]. D. R. Rani and G. Geethakumari (2015). An efficient approach to forensic investigation in cloud using VM snapshots. *In 2015 International Conference on Pervasive Computing (ICPC)*, 1–5.

[10]. S. Khan, M. Shiraz, A. W. Abdul Wahab, A. Gani, Q. Han, and Z. Bin Abdul Rahman (2014). A Comprehensive Review on Adaptability of Network Forensics Frameworks for Mobile Cloud Computing. *Sci. World J.*, 1–27.

[11]. M. Damshenas, A. Dehghantanha, R. Mahmoud, and S. bin Shamsuddin (2012). Forensics investigation challenges in cloud computing environments. In Proceedings Title: *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, 190–194.

[12]. B. Martini and K.-K. R. Choo (2013). Cloud storage forensics: ownCloud as a case study. *Digit. Investig., 10*(4), 287–299.

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

[14]. D. Quick and K. K. R. Choo (2014). Google Drive: Forensic analysis of data remnants. *J. Netw. Comput. Appl., 40*, 179–193.

[15]. S. Easwaramoorthy, S. Thamburasa, G. Samy, S. B. Bhushan, and K. Aravind (2016). Digital forensic evidence collection of cloud storage data for investigation. *In 2016 International Conference on*

Recent Trends in Information Technology (ICRTIT), 1–6.
[16]. S. Simou, C. Kalloniatis, S. Gritzalis, and H. Mouratidis (2016). A survey on cloud forensics challenges and solutions. *Secur. Commun. Networks, 9*(18), 6285–6314.
[17]. M. E. Alex and R. Kishore (2017). Forensics framework for cloud computing. *Comput. Electr. Eng., 60*, 193–205.
[18]. B. K. S. P. K. Raju and G. Geethakumari (2016). An advanced forensic readiness model for the cloud environment. *In 2016 International Conference on Computing, Communication and Automation (ICCCA)*, 765–771.
[19]. Khan, S., Gani, A., Wahab, A. W. A., Bagiwa, M. A., Shiraz, M., Khan, S. U., & Zomaya, A. Y. (2016). Cloud log forensics: Foundations, state of the art, and future directions. *ACM Computing Surveys (CSUR)*, *49*(1), 1-42.
[20]. B. Hay, K. Nance, and M. Bishop (2011). Storm Clouds Rising: Security Challenges for IaaS Cloud Computing. *In 2011 44th Hawaii International Conference on System Sciences,* 1–7.
[21]. K. Ruan and J. Carthy (2013). Cloud Computing Reference Architecture and Its Forensic Implications: A Preliminary Analysis, 1–21.
[22]. T. Sang (2013). A Log Based Approach to Make Digital Forensics Easier on Cloud Computing. *In 2013 Third International Conference on Intelligent System Design and Engineering Applications,* 91–94.
[23]. Pichan, M. Lazarescu, and S. T. Soh (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. *Digit. Investig.*, *13,* 38–57.
[24]. D. Liu, J. Lee, J. Jang, S. Nepal, and J. Zic (2010). A Cloud Architecture of Virtual Trusted Platform Modules. *In 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing,* 804–811.
[25]. W. Delport and M. Olivier. (2012). *Isolating Instances in Cloud Forensics,* 187–200.
[26]. J. Dykstra and A. T. Sherman (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digit. Investig.*, *9,* S90–S98.
[27]. Zawoad, S. & Hasan, R. (2013). Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. CoRR, abs/1302.6312.
[28]. Poisel, R., Malzer, E., & Tjoa, S. (2013). Evidence and Cloud Computing: The Virtual Machine Introspection Approach. J. Wirel. Mob. Networks Ubiquitous Comput. *Dependable Appl., 4*, 135-152.
[29]. Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., & Lee, B. S. (2011). TrustCloud: A framework for accountability and trust in cloud computing. In *2011 IEEE World Congress on Services* (pp. 584-588).
[30]. M. Alhamad, T. Dillon, and E. Chang (2010). Conceptual SLA framework for cloud computing. *In 4th IEEE International Conference on Digital Ecosystems and Technologies,* 606–610.
[31]. Adhianto, L., Banerjee, S., Fagan, M., Krentel, M., Marin, G., Mellor-Crummey, J., & Tallent, N. R. (2010). HPCToolkit: Tools for performance analysis of optimized parallel programs. *Concurrency and Computation: Practice and Experience*, *22*(6), 685-701.
[32]. S. Almulla, Y. Iraqi, and A. Jones (2014). A State-Of-The-Art Review of Cloud Forensics. *J. Digit. Forensics, Secur. Law*.
[33]. E. Morioka and M. S. Sharbaf (2015). Cloud Computing: Digital Forensic Solutions. *In 2015 12th International Conference on Information Technology - New Generations*, 589–594.
[34]. Bamane, K. (2019). A Study of Cloud Forensics: Technical Issues, Challenges, Tools and Technologies. *IJETT, 6*(3).
[35]. Jain, P., & Mahalkari, A. (2019). Review of Cloud Forensics: Challenges, Solutions and Comparative Analysis. *International Journal of Computer Applications*, *975*, 8887.
[36]. Manral, B., Somani, G., Choo, K. K. R., Conti, M., & Gaur, M. S. (2019). A systematic survey on cloud forensics challenges, solutions, and future directions. *ACM Computing Surveys (CSUR)*, *52*(6), 1-38.

How to cite this article: Yassin, W., Baharon, M. R., Bahaman, N., Abas, Z. A. and Abdollah, M. F. (2020). A Review of Cloud Forensic Investigation: Challenges, Recommendation and Readiness. *International Journal on Emerging Technologies, 11*(5): 98–105.