Editorial

ICSES Interdisciplinary Transactions on Cloud Computing, IoT, and Big Data (IITCIB)

Journal Homepage: http://www.i-cses.com/iitcib

The Challenges of Forensic Investigation in Cloud

W. Yassin *

Faculty of Information and Communications Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

* Corresponding Author: s.m.warusia@utem.edu.my

THE emerging technology of cloud computing, receiving much popularity as the resources shared widely at anytime and anywhere [1]. However, at the same time, it also opens an opportunity to research community to discover a solution as massive vulnerabilities in it causes cybercrime. Instead, digital forensic investigation also has no exception in facing much challenges even though this method of investigation widely practiced and applied approximately thirty years ago. In these innovative modern computing environments, the major challenges to conduct a forensic investigation are in a process of data collection, integrity of evidence as the sources could be from a different location, format issues and so forth. As utilization of cloud computing services keep growing and could increase the cybercrime it is necessary to highlight the challenges and recommendation within the field of forensic for future consideration.

The common definition of cloud computing can be referred as procedure of pooling and sharing the computing resources at a distance in an aim such resources can be accessed at anytime and anywhere. However, the NIST has defined the cloud computing term into "cloud computing is a model that enable ubiquitous, convenient, on-demand network access to a shared pool computing resources, i.e. networks, applications, set of servers, storage and services which can be frequently provide and delivered with minimum management exercise or service provider interaction" [2], [3]. In addition, NIST has come with basic cloud model, whereas the model comprises four deployment models of cloud such as public, private, hybrid and community. Furthermore, the model also divided into three major services, i.e. Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). On-demand self-service, broad network access, resource pooling, rapid elasticity and measured service is illustrated as the core essential characteristic of the cloud model. Moreover, the core technology, which enables cloud facilities are virtualization [4]. Unfortunately, the client has limited privileges on their rental services as well as the location of such services are unknown except to the Cloud Service Provider (CSP). For example, SaaS is fully controlled by CSP as the client only abilities to store and retrieve the data.

The significant developments in cloud computing could be benefiting the client as it is possessed certain benefits, however, if the technology is not focused on perspective of the security requirement, it will directly affect the forensic investigation activities to be difficult as well as directly increasing the amount of cybercrime. As stated in [5], the process of forensic investigation against the cloud computing resources such as networks, servers and any acceptable sources are known as cloud forensic. Based on literature study, the most important principles that need to be considered in forensic challenges is the limited privileges given by CSPs to the client in controlling the cloud resources, the invisibility of the cloud to others and law enforcement.

There are various cloud forensic models that comprises several phases has been proposed by a number of research community. The major phases can be summarized as identification, collection and preservation, examination and analysis, and reporting and presentation. Each phase has their own drawback that could not feed to conduct forensic investigation.

Usually the process of crime or cyber threat activity identification involve in identification phase, which comprises several sub-component such as incident identification, evidence identification and evidence location [6]. Regrettably, in the cloud computing ecosystem, an appropriate logs information for incident and evidence identification are limited as the client does not have any privileges to access it beside the nature of cloud embedded in distributed location. In addition, as the virtual machine have certain circumstances, such as volatile when log off and fully controlled by the CSP, it is difficult to obtain the evidence after termination of the virtual machine [7].

On the other hand, the collection (also known as acquisition) and preservation phase concern for evidence preservation, acquire the data forensically, preserve the artifacts and the way the data collected. This phase also can be referred as a process of data or evidence collection without losing the integrity of the data and then examine it through a sort of related tools. Unfortunately, it is difficult to maintain the integrity of data or evidence [8] as it is volatile in nature whereas the original data have changed and valueless in front of the law, and acquiring physical access to the cloud is impossible as it is prohibited by CPSs.

The examination and analysis phase usually relate with the process of examination and analysis of data and draft conclusion. Using conventional analysis on a dedicated network, usually this phase associate with correlation of multiple sources to justify or verify the evidences is not touchable or altered. However, the resources on the cloud normally shared by multiple clients and cause the evidence distribute around numerous location. Consequently, it is difficult for the investigator to perform analysis and draw the conclusion.

Presentation is the final phase in forensic in which this process much easier in digital forensic as a contrast to cloud forensic. This is because with thousands of VMs running simultaneously via thousands of clients on cloud data center could create a critical risk for evidence gathering that will pose huge challenges. Thus, is very hard for the forensic investigator to represent the appropriate evidence as a report at the court [9].

Referring to the identification phase, the logging concept for gathering evidence could be beneficial to the forensic investigation. For example, in [10] have proposed logging method to cloud environment to monitor the behavior of connected virtual machines. These methods able to capture useful information such as time frame, attacker IP's, browser information and so forth. Moreover, in [11] also has proposed such logging method for SaaS and PaaS. In this work, third party component has utilized to produce logs for the cloud and clients. In addition, this approach has reduced the verification time and enhance its efficiency.

Apart from this, some focused has been given in recommending solutions for collection and preservation phase. For instance, in order to authorize client as well as secure the integrity of the evidence [12] virtual private network, which enabling authentication method [13] and cryptographic tunneling protocol function has considered. Furthermore, the public key infrastructure really helps the investigator in identifying the victim.

Besides, for examination and analysis phase, a number of researchers have highlighted that there is a challenges of lack of cloud forensic tools. In 2011, the Black Hat has introduced offline Windows Analysis and Data Extraction (OWADE) specifically for cloud user to extract the entire information stored inside the cloud. Similarly, FORST has proposed to extract information of API logs, virtual disk and firewall logs and became the initial IaaS model forensic tool [8]. Furthermore, another researcher in [14] has proposed the investigator to re-run the attack after snapshot the original state of the system. So that, the previous activity perform by the attack can be examined and analyze. As the above three phase's challenges can be solved throughout the recommended solution, the presentation and reporting phase could be easier.

The cloud computing technology is still under the progress element in which the security perspective still needs to be improved, so that the forensic investigation could be performed easily. There are various challenges that need to be faced by the forensic investigator currently such as identification and evidence collection circumstances, difficulties in analyzing the evidence as well as convey such evidence for law enforcement. That is the reason this article focuses on highlighting the challenges and give some recommendation as a solution.

With Regards
Dr. Warusia Mohamed Yassin
30 March 2018
Warusia

Warusia Mohamed Yassin is a senior lecturer in Department of Computer Systems and Communication at the Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka (UTeM). He is a member of information security, digital forensic and computer networking (INSFORNET) research group. He completes his Bachelor Degree in Computer Science (2008), Master of Science (2011) and PhD (2015) at Universiti Putra Malaysia (UPM). His research interests include Security In Computing, Machine Learning and Cloud Computing.

REFERENCES

[1] F. Zafar et al., "A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends," *Comput. Secur.*, vol. 65, pp. 29–49, 2017. DOI: 10.1016/j.cose.2016.10.006

[2] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey*," Futur. Gener. Comput. Syst.*, vol. 56, pp. 684–700, 2016.DOI: 10.1016/j.future.2015.09.021

[3] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," *Nist Spec. Publ.*, vol. 145, p. 7, 2011.

[4] F. Sabahi, "Cloud computing security threats and responses," in proc. *2011 IEEE 3rd International Conference on Communication Software and Networks*, pp. 245–249, 2011. DOI: 10.1109/ICCSN.2011.6014715

[5] K. Ruan and J. Carthy, "Cloud Computing Reference Architecture and Its Forensic Implications: A Preliminary Analysis," in proc. *Digital Forensics and Cyber Crime*, pp. 1–21, 2013.

[6] A. Pichan, M. Lazarescu, and S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," *Digit. Investig.*, vol. 13, pp. 38–57, 2015. DOI: 10.1016/j.diin.2015.03.002

[7] D. R. Rani and P. L. Sravani, "Challenges of digital forensics in cloud computing environment," *Indian J. Sci. Technol.*, vol. 9, no. 17, 2016. DOI: 10.17485/ijst/2016/v9i17/93051

[8] J. Dykstra and A. T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques," *Digit. Investig.*, vol. 9, pp. S90–S98, Aug. 2012. DOI: 10.1016/j.diin.2012.05.001

[9] R. Marty, "Cloud application logging for forensics," in Proc. *2011 ACM Symposium on Applied Computing - SAC '11*, pp. 178, 2011. DOI: 10.1145/1982185.1982226

[10] Zafarullah, F. Anwar, and Z. Anwar, "Digital Forensics for Eucalyptus," in proc. *2011 Frontiers of Information Technology*, pp. 110–116, 2011.

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

[12] S. Alqahtany, N. Clarke, S. Furnell, and C. Reich, "A forensic acquisition and analysis system for IaaS," *Cluster Comput.*, vol. 19, no. 1, pp. 439–453, Mar. 2016. DOI: 10.1007/s10586-015-0509-x

[13] P. S. Kumari and A. R. N. B. Kamal, "Optimal Integrity Policy for Encrypted Data in Secure Storage using Cloud Computing," *Indian J. Sci. Technol.*, vol. 9, no. 8, Mar. 2016. DOI: 10.17485/ijst/2016/v9i8/87923

[14] G. Geethakumari and A. Belorkar, "Regenerating Cloud Attack Scenarios using LVM2 based System Snapshots for Forensic Analysis*," Int. J. Cloud Comput. Serv. Sci.*, vol. 1, no. 3, pp. 134–141, 2012. DOI: 10.11591/closer.v1i3.803