2020 International Conference on Information Technology Systems and Innovation (ICITSI)
Bandung - Padang, October 19 - 23, 2020
ISBN: 978-1-7281-8196-7

Design Framework Forensics Readiness as a Service for Automatic Processing

Samuel Andi Kristyan[1], Suhardi[2], Tutun Juhana[3]
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
muelandi@gmail.com[1], suhardi@stei.itb.ac.id[2], tutun@stei.ac.id[3]

***Abstract*— Cloud computing technologies are one of the most developed knowledge fields today. However, the rapid growth of cloud computing has made cybercrime crime grow. This poses new challenges to investigating. Currently, there have been many research models and frameworks that support the forensics investigation process and methodology, but the existing frameworks are not suitable to be implemented automatically in a cloud environment. By using a literature survey, the researcher proposes a model that can be applied to a cloud environment. The proposed model is expected to carry out investigations automatically and aims to maximize the use of digital evidence so that readiness can be achieved.**

Keywords—forensics readiness, cloud computing, forensics readiness as a service

I. INTRODUCTION

Cloud services are elastic, which means they are released based on the demands of user scaling. The service runs on a cloud infrastructure which can consist of several machines in different geographic zones without accurate routing information; resources were virtualized using Virtual Machine Management (VMM)[1]. This flexibility results in reduced access to physical control of the cloud computing architecture components.

Investigating the use of cloud computing by criminals or victims of crime presents its challenges because the devices used are virtualized and geographically distributed among jurisdictions. The technical challenge that arises is the stages of identification and seizure by law enforcers, which can hinder investigations and potentially prevent law enforcement and national security agencies from obtaining digital evidence and analyzing digital content in a timely manner[2]. The stage for obtaining digital evidence is commonly called digital forensics, which is the stage used to investigate crimes against digital devices to activate crime or as targets of crime.

The difference between traditional digital forensics frameworks and cloud forensics is the acquisition stage where the traditional digital forensics framework is focused on taking evidence on physical devices. Meanwhile, in cloud forensics, the acquisition cannot be done on a physical device. Cloud Forensics framework and model is a method of forensic data preservation and cloud computing data collection for forensic purposes[3]. Currently, there is no standard framework and model that can be applied properly for the investigation process because the investigation process depends on the area of investigation and the case. The framework used during the investigation process can be classified based on the number of stages used. The two most widely used and accepted forensic frameworks are McKemmish 1999[4] and NIST 2006[5]. To date, various frameworks and models have been proposed in the digital forensics field. But existing frameworks can be well implemented in non-cloud environments. In the case of the cloud, no framework can be implemented automatically and reduce human interaction. This research will propose a model that can be applied automatically in a cloud environment.

II. RELATED WORK

A digital forensics framework is a process model or methodology used to guide the investigation process[6]. Currently, the proposed framework in digital forensics focuses on specific stages of digital forensics, such as identification, collection, preservation, and examination analysis[7], [8].

Many frameworks are proposed in various fields of digital fields, such as in digital forensics in general, computer forensics, IoT forensics, network forensics, mobile forensics, and cloud forensics. Each proposed framework has different characteristics such as the strategy used for evidence gathering and the number of stages used to carry out investigations based on the implementation area[3]. The digital forensic framework can be defined as structured stages to support forensic investigations. This implies that the conclusions reached by one computer forensic expert must be the same as that of others who have conducted investigations using the same framework[9]. The digital forensics framework generally consists of each of the following steps:

Table 1 Digital Forensics framework

Author	Identification stage	Examination and analysis stage	Evidence Acquisition, Collection, and preservation.	Presentation and reporting stage
B. Martini 2012, et al [3]	V	V	V	V
M. Khanafseh, et al 2019 [6]	V			
D. Vadlamudi, et al 2018 [10]	V	V	V	V
J. J. Shah, et al 2014 [11]	V	V	V	V
R. C. Hegarty, et al 2014 [12]	V	V		V
S. Alqahtany, et al 2015 [13]	V	V	V	V
B. Manral, et al 2019 [14]	V	V	V	V
P. K. Keserwani, et al 2017 [15]	V	V	V	V
J. Jain, et al 2020 [16]	V	V		
S. Alqahtany, et al 2016 [17]	V		V	V
S. Bhatia, et al 2019 [18]	V			V

Authorized licensed use limited to: Universiti Kebangsaan Malaysia. Downloaded on January 31,2021 at 03:21:49 UTC from IEEE Xplore. Restrictions apply.

Author	Identification stage	Examination and analysis stage	Evidence Acquisition, Collection, and preservation.	Presentation and reporting stage
T. Zia, et al 2017 [19]		V	V	V
B. K. S. P. K. Raju, et al 2016 [20]		V	V	
B. Carrier, et al 2004 [21]				V
J. Farina, et al 2015 [22]				V

The previously surveyed framework works well with non-cloud digital devices manually. Barrett and Kipper (2010) suggest that the existing digital forensic methods are not suitable for cloud computing environments[23]. Therefore, some adjustments are needed. Several researchers have proposed frameworks aimed at cloud environments, including Martini 2012[3] and Sachowski 2016[24]. Cloud Forensics framework is a method of forensic data preservation and cloud computing data collection for forensic purposes[3].

The digital forensics technique itself is divided into two, namely proactive and reactive[25]. Reactive digital forensics is forensics for something that has happened later, retrospectively, doing postmortem, and analyzing behavior and recording what can be learned to prevent the event from happening again in the future. Meanwhile, proactive (forensics readiness) is a stage that must be prepared before an incident occurs. In 2018 Kristyan[26] surveyed the components of forensics readiness. From the survey results, there are still a few models that propose technical aspects for forensics readiness.

The stages for digital forensics and forensics readiness are almost the same. It is a challenge if you want to implement a framework on cloud computing devices automatically. Therefore it is necessary to propose a framework that can be applied to cloud computing automatically, where the involvement of human roles is minimized. This study will modify several forensics methods in order to achieve readiness and be implemented in a cloud environment.

III. Proposed Model

From the stages of the literature survey that has been carried out above, it shows that the existing framework or methodology is effective in searching for manual evidence that requires human involvement in every stage. Therefore, it is necessary to propose a framework that can be automated in every stage. The proposed framework aims to reduce human interaction at every stage.

Based on the existing framework, the authors propose four stages of forensics readiness that can be implemented in cloud computing. The difference between the existing and the proposed stages is that there are repeated stages to collect evidence from the results of the analysis. The four stages are as follows:

a. Identification
   This phase is concerned with identifying types of attacks such as web hacking, malware, and others. This stage will identify what assets are related to the type of attack. This stage also explains what data sources will be taken. This stage is decisive because each attack has a different data source. This stage aims to reduce the volume of data captured.
b. Gathering
   This stage is concerned with gathering evidence centrally before or after the vulnerability analysis. Evidence collection and after vulnerability checks are intended to speed up checking in the event of a security incident. This stage can be carried out within the jurisdiction with the aim that the evidence obtained does not cross the applicable law. At this stage, besides the evidence taken, there is also a sub-stage of collecting vulnerability databases from public databases such as Mitre. Vulnerability database functions to check existing vulnerabilities.

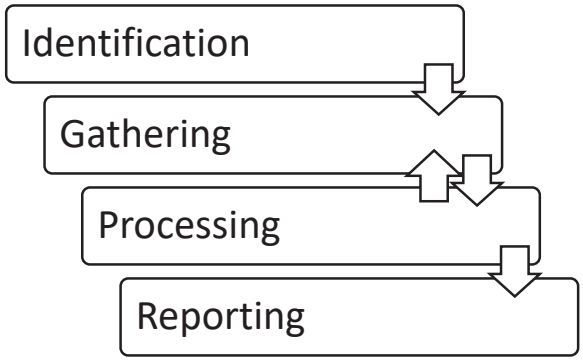

Figure 1 framework digital forensics readiness

c. Processing
   This stage is the stage of checking for vulnerabilities. Several machine learning methods can be applied at this stage. The result of this stage is an existing vulnerability map. From this vulnerability map, it will then return to the gathering stage, namely the collection of related artifacts that can become evidence. Returning the process to a gathering is aimed at achieving readiness.
d. Reporting
   This stage is the stage of reporting on the evidence or vulnerability that has been found. The reporting stages can be seen by the customer and the provider, then the reporting provider can provide input to the customer.

The process model developed to support cloud digital forensics readiness is somewhat different from the framework developed for digital forensic investigation workflows. The process model for cloud digital forensics readiness consists of activities and steps in an iterative hierarchy, especially for gathering and processing stages. According to Sachowski 2016[24], the cloud digital forensics readiness process model aims to form a technical foundation that effectively supports the activities and tasks performed in all phases of the following digital forensics readiness framework:

- Minimizing digital forensic investigation costs.
- Maximize the potential use of digital evidence.
- Minimizing disruption of business processes.
- Speed up investigations.
- Maintain and improve information security posture.

Sachowski himself has proposed a derivative model from the existing four-stage framework. But the proposed model is not yet intended for automatic processing. The proposed

Authorized licensed use limited to: Universiti Kebangsaan Malaysia. Downloaded on January 31,2021 at 03:21:49 UTC from IEEE Xplore. Restrictions apply.

model still requires management interaction. The four stages of the model proposed by Sachowski 2016 are:

1. Preparation
   - Scenario definition
   - Collection requirement
   - Preservation requirement
   - Management requirement
   - Escalation requirement
   - Resource planning
2. Gathering
   - Identify sources
   - Data collection
   - Data preservation
3. Processing
   - Continuous monitoring
   - Digital forensics process model
   - Legal review
4. Presentation
   - Evidence based presentation

Based on the Sachowski 2016 framework model, the authors made modifications so that the implemented framework model could automate the cloud environment. This is the framework model that the authors propose.

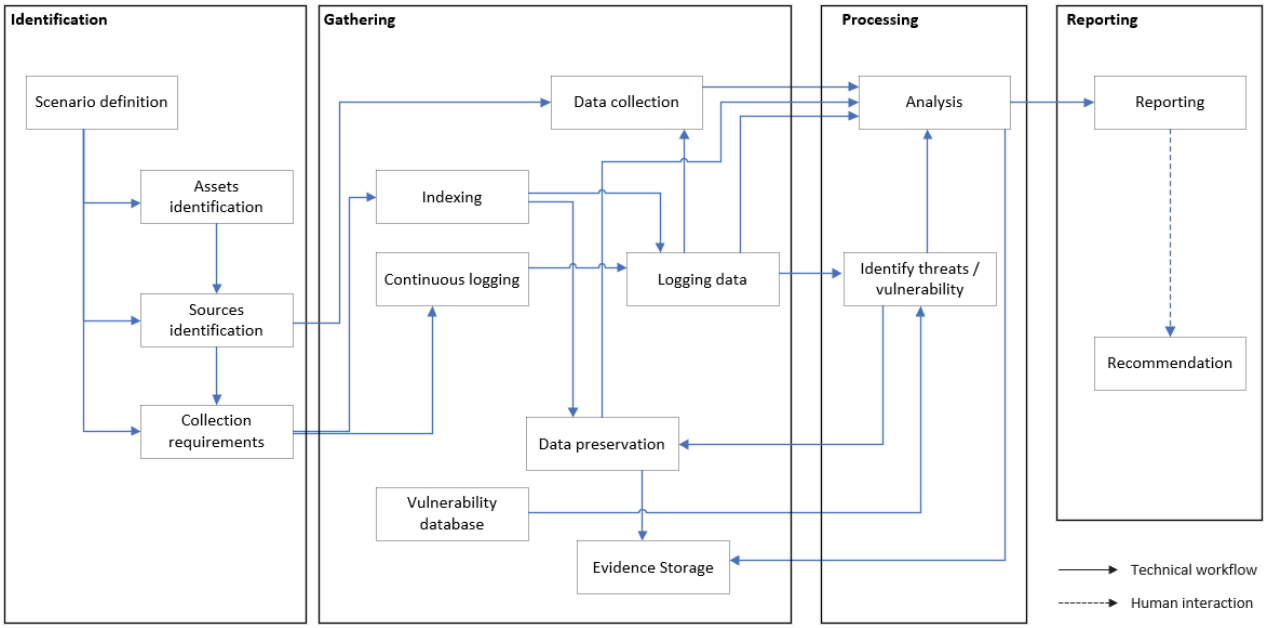

Figure 2 digital forensics readiness as a service framework model

Figure 2 illustrates the activities and steps that make up the cloud forensics digital readiness as a service model. The definition of the sub-stages is:

a. Scenario definition: this stage is the stage of identifying the type of attack that will occur. The choice of attack will determine the type of data and assets to be checked, such as malware will be focused on checking RAM and hard disk, while for web hacking checks will be focused on checking logs and also access. At this stage, a database will be provided that contains the types of attacks that are common.

b. Assets identification: this stage is the stage of identifying assets associated with an attack. Each possible attack will have a different set of assets to examine. For example, in a malware attack, the assets examined are servers and routers. The purpose of asset limitation is to reduce the volume of data to be examined to shorten the time of the investigation. At this stage, a database will be provided which contains a list of assets related to the type of attack.

c. Sources identification: is the stage of identifying the data source of the assets related to the attack (RAM, hard disk, OS, etc.). Examples of malware attacks, then the data sources that are checked are RAM, HDD, OS, etc. This stage itself is intended so that the examination volume can be reduced again.

d. Collection requirements: this stage identifies what can be taken and used as evidence, such as application logs, access control logs, OS logs, network logs, etc.

e. Data collection: is the acquisition stage, namely the stage of taking raw sources to be analyzed and extracted. For example, contents of memory, contents of hard disk, data traffic on the network, etc.

f. Indexing: this stage is the stage of extracting data. For example, the contents of RAM become a list of application logs, or the contents of a hard disk become a data list of artifacts and their locations. This stage usually requires a large enough computation to speed up the extraction because the larger the data size, the more data that must be extracted in detail. The output of this stage is the timeline. This timeline will then be examined at the analysis stage.

g. Continuous logging is the stage of logging every time there is a change to the real-time system. Data that is recorded in real-time can be log data. The result of this stage is the timeline, different from the indexing stage, which is usually done once, this stage will record continuously.

h. Vulnerability database: the stage of collecting vulnerability data from external databases such as partners. This database will make regular updates every day so that the vulnerability data it has are valid.

Authorized licensed use limited to: Universiti Kebangsaan Malaysia. Downloaded on January 31,2021 at 03:21:49 UTC from IEEE Xplore. Restrictions apply.

i. Data preservation: the stage of taking data after a vulnerability is identified. This stage is the core of forensics readiness because at this stage the platform will collect artifacts that are vulnerable to attack so that the customer can maximize evidence. Collected artifacts will be immediately available as soon as there is a security incident so that the forensics readiness objectives above can be achieved.

j. Logging data: data obtained from indexing and continuous logging in the form of a timeline. Logging data is a centralized database that will be examined by the analysis stage.

k. Evidence storage: the stage of storing evidence from the results of the analysis. This step is also useful for storing other VM evidence. Data evidence is stored in jurisdictions so as not to violate applicable laws.

l. Analysis: exploitation stages of the existing vulnerability list. This stage aims to find evidence of vulnerabilities that can be exploited. Artifacts that can be exploited are then stored in evidence storage as evidence. Also, if there is a vulnerability that can be exploited, the system will send a notification to the reporting section.

m. Identify threats / vulnerability: stages of identifying threats/vulnerabilities with timeline data and vulnerability database data. Several machine learning methods can be applied at this stage so that vulnerabilities can be mapped properly. The success of this stage will be largely determined by the vulnerability database that is owned.

n. Reporting: the stage of notification once the vulnerability appears. The notification that appears will be sent to both the customer and the provider. Providers here are experts who can provide information and recommendations to clients about what happened and how to handle it.

o. Recommendation: the stages of proposals that must be carried out. The proposal involves DFRaaS provider to customers. This proposal requires expert interaction.

In this proposed model, there is a combination of sequential and iterative steps in each phase. The proposed sub-stages are intended to be automated. The proposed model is expected to meet the objectives of forensics readiness namely, to make maximum use of evidence so that it can speed up investigations without disrupting business processes. In the next study, the authors will develop a system that aims to test the proposed model.

IV. Conclusion

The increasing use of cloud services brings with it an increasing number of cyber threats. This poses technical challenges for digital investigations. Hence, security in the cloud should be taken seriously. Although the cloud environment has become an interesting battleground for cybercrime, there is very little research on forensics readiness in the cloud environment that addresses the technical side. The research found that cloud readiness can be automated to be implemented in a cloud environment. This paper has mapped and identified the stages influencing the readiness of forensics using cloud services. The next research plan is to develop a forensics readiness platform on the cloud based on the cloud forensics readiness as a service model.

References

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Gaithersburg, MD, 2011. doi: 10.6028/NIST.SP.800-145.

[2] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digit. Investig.*, vol. 7, pp. S64–S73, Aug. 2010, doi: 10.1016/J.DIIN.2010.05.009.

[3] B. Martini and K. K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digit. Investig.*, vol. 9, no. 2, pp. 71–80, 2012, doi: 10.1016/j.diin.2012.07.001.

[4] R. Mckemmish and A. Graycar, "What is Forensic Computing?," *Aust. Inst. Criminol.*, 1999, Accessed: Jun. 23, 2020. [Online]. Available: http://www.aic.gov.au.

[5] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," Gaithersburg, MD, 2006. doi: 10.6028/NIST.SP.800-86.

[6] M. Khanafseh, M. Qatawneh, and W. Almobaideen, "A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 8, pp. 610–629, 2019.

[7] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *Digit. Investig.*, vol. 7, no. 1–2, pp. 14–27, Oct. 2010, doi: 10.1016/j.diin.2010.02.003.

[8] M. Kohn, J. Eloff, and M. S. Olivier, "Framework for a Digital Forensic Investigation," 2006.

[9] Gary Palmer, "A Road Map for Digital Forensic Research," *Digit. Forensics Res. Conf.*, 2001, doi: 10.1016/0032-3950(82)90064-8.

[10] D. Vadlamudi, K. Thirupathi Rao, P. Vidyullatha, and B. RajasekharReddy, "Analysis on digital forensics challenges and anti-forensics techniques in cloud computing," *Int. J. Eng. Technol.*, vol. 7, no. 2.7 Specia, pp. 1072–1075, 2018.

[11] J. J. Shah and L. G. Malik, "An approach towards digital forensic framework for cloud," in *2014 IEEE International Advance Computing Conference, IACC 2014*, 2014, pp. 798–801, doi: 10.1109/IAdCC.2014.6779425.

[12] R. C. Hegarty, D. J. Lamb, and A. Attwood, "Digital evidence challenges in the internet of things," in *Proceedings of the 10th International Network Conference, INC 2014*, 2014, pp. 163–172.

[13] S. Alqahtany, N. Clarke, S. Furnell, and C. Reich, "Cloud Forensics: A Review of Challenges, Solutions and Open Problems," *2015 Int. Conf. Cloud Comput. ICCC 2015*, no. April, 2015, doi: 10.1109/CLOUDCOMP.2015.7149635.

[14] B. Manral, G. Somani, K.-K. R. Choo, M. Conti, and M. S. Gaur, "A systematic survey on cloud forensics challenges, Solutions, and future directions," *ACM Comput. Surv.*, vol. 52, no. 6, 2019, doi: 10.1145/3361216.

[15] P. K. Keserwani and S. G. Samaddar, "Customization of Service Level Agreement for Digital Forensics as a Service," *ACM Int. Conf. Proceeding Ser.*, pp. 139–150, 2017, doi: 10.1145/3154979.3154993.

[16] J. Jain and A. Singh, "Quantum-based Rivest-Shamir-Adleman (RSA) approach for digital forensic reports," *Mod. Phys. Lett. B*, vol. 34, no. 6, 2020, doi: 10.1142/S0217984920500852.

[17] S. Alqahtany, N. Clarke, S. Furnell, and C. Reich, "A forensic acquisition and analysis system for IaaS: Architectural model and experiment," in *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, Dec. 2016, pp. 345–354, doi: 10.1109/ARES.2016.58.

Authorized licensed use limited to: Universiti Kebangsaan Malaysia. Downloaded on January 31,2021 at 03:21:49 UTC from IEEE Xplore. Restrictions apply.

[18] S. Bhatia and J. Malhotra, "Forensic Based Cloud Computing Architecture-Exploration and Implementation," in *2019 Proceedings of the 3rd International Conference on Computing and Communications Technologies, ICCCT 2019*, 2019, pp. 37–45, doi: 10.1109/ICCCT2.2019.8824813.

[19] T. Zia, P. Liu, and W. Han, "Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT)," 2017, doi: 10.1145/3098954.3104052.

[20] B. K. S. P. K. Raju and G. Geethakumari, "An advanced forensic readiness model for the cloud environment," *Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2016*, pp. 765–771, 2017, doi: 10.1109/CCAA.2016.7813819.

[21] B. Carrier and E. Spafford, "An Event-Based Digital Forensic Investigation Framework," 2004.

[22] J. Farina, M. Scanlon, N.-A. Le-Khac, and M.-T. Kechadi, "Overview of the forensic investigation of cloud services," in *Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015*, 2015, pp. 556–565, doi: 10.1109/ARES.2015.81.

[23] D. Barrett and G. Kipper, *Virtualization and forensics*. 2010.

[24] J. Sachowski, *Implementing Digital Forensic Readiness: From Reactive to Proactive Process*. 2016.

[25] S. Alharbi, J. Weber-Jahnke, and I. Traore, "The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review," *Int. J. Secur. Its Appl.*, vol. 5, no. 4, 2011, doi: 10.1007/978-3-642-23141-4.

[26] S. A. Kristyan and Suhardi, "Forensics Readiness survey in cloud computing with a meta-analysis approach," in *2018 International Conference on Information Technology Systems and Innovation, ICITSI 2018 - Proceedings*, 2018, pp. 574–581, doi: 10.1109/ICITSI.2018.8695992.

Authorized licensed use limited to: Universiti Kebangsaan Malaysia. Downloaded on January 31,2021 at 03:21:49 UTC from IEEE Xplore. Restrictions apply.