International Journal of Engineering & Technology, 7 (4.15) (2018) 7-11

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Digital Forensic Investigation Challenges based on Cloud Computing Characteristics

Ganthan Narayana Samy[1]*, Nurazean Maarop[1], Mohd Shahidan Abdullah[1], Sundresan Perumal[2], Sameer Hasan Albakri[1], Bharanidharan Shanmugam[3], Premylla Jeremiah[1]

[1]Advanced Informatics School, Universiti Teknologi Malaysia, Malaysia
[2]Faculty of Science and Technology, Universiti Sains Islam Malaysia, Malaysia
[3]School of Engineering and Information Technology, Charles Darwin University, Australia
**Corresponding author E-mail: ganthan.kl@utm.my*

Abstract

One of the most popular computing technologies is cloud computing. There are many benefits in adopting cloud computing such as high-performance, flexibility and availability on-demand, more focused on the business objective and low-cost. However, the characteristics of the cloud computing environment have created many difficulties and challenges for digital forensic investigation processes. Therefore, this paper focuses on the digital forensic investigation challenges based on cloud computing characteristics.

Keywords: *Cloud Computing Characteristics; Cloud Computing Forensics; Digital Forensics Challenges; Digital Forensics Processes.*

1. Introduction

One of the most popular computing technologies is cloud computing. There are many benefits of cloud computing, such as high-performance, flexibility and availability on-demand, more focused on the business objective, and low-cost. The main concept of cloud computing is providing the computing services based on the virtualization that provides better utilization of computer resources. The cloud computing service providers are delivering computing implementations as services, the end user can access these services when needed and pay per usage. Cloud computing is a cost effective for medium and small scale organizations, in which they do not need to build their own physical computing infrastructures [1].

Not only the legitimate individual users and organizations are benefiting from the development of technology, but also the criminals have greatly benefited from the speed internet and cloud computing services to commit their crimes and build collaboration network between criminals [2]. Moreover, there are many security concerns in the cloud computing environments such as abusing cloud computing services and tools, improper usage of the access authorizations, cracking passwords, and launching DoS and DDoS attacks. Technologies that used by cloud service providers to build their cloud computing infrastructure may bring some security concerns. For instance, virtualization technology, which is a technology that enable the cloud service provider to use same physical infrastructure to serve multiple users at the same time. There are many security threats that might accompany the use of virtualization technology such as the potential of data leaks in the virtualization software layer and the users' data isolation [3].

The normal procedure when a crime is committed by using a digital equipment is conducting a digital forensic investigation. The digital forensic investigation aims to extract the sound evidence about the crime from the digital equipment. The characteristics of the cloud computing environment have created many difficulties and challenges for digital forensic process. In fact, cloud computing has multi-stakeholders and this leads to responsibilities overlapping that make digital forensic processes in cloud computing more complex [4]. Usually, cloud service providers build their data centers in different geographic locations, which add more challenges for the digital forensic processes [5].

Unlike traditional computing environment, where seizing the digital device that used in a digital crime is easy, the process of isolating and acquiring the digital device in a cloud computing environment is very complicated and even impossible to perform similarly as in the traditional computing environment [5]. This complexity aroused from the fact that the physical computing resources are shared between the cloud computing customers and the fact that data centers exists in different geographical places and may be under different jurisdictions. The ultimate goal for any digital forensic investigation is to find a potential evidence to be used at court, the digital forensic investigators have to search, preserve, and analyze information on computer systems to come out with sound and solid evidence. However, it is difficult to follow the traditional digital forensic investigation process in the cloud computing environment because the data stored on it would be encrypted or split across multiple computer systems.

This paper focuses on the cloud computing characteristics that increase the complexity of the digital forensic processes in the cloud computing environment. Section 2 introduces a brief discussion for cloud computing environment. Section 3 mentions the main challenges of the cloud digital forensic briefly. A discussion of these challenges in each digital forensic investigation is presented in Section 4 and finally, Section 5 concludes this paper.

2. Cloud Computing Environment

Different definitions for cloud computing have been introduced for cloud computing, in which each researcher has introduced cloud computing model based on his study point of view. ISO/IEC 17788:2014 define the cloud computing as follow, "Cloud Computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand" The report defines the Cloud Computing Provider as "a natural person or legal person, whether or not incorporated, or a group of either, which makes cloud services available", and the Cloud Computing Customer as "a natural person or legal person, whether or not incorporated, or a group of either which is in a business relationship for the purpose of using cloud services". Moreover, it defines the Service Level Agreement (SLA) as "a documented agreement between the service provider and customer that identifies services and service targets" [6].

Despite cloud computing being seen as a new approach for delivering computing services, a kind of unstandardized distributed systems, or a high level of IT outsourcing, cloud computing is expected to become the most common computing model. Cloud computing has many advantages. For instance, it reduced the computing cost and enable the cloud customers to overcome of the limits of time and place [7]. However, cloud computing services are delivered on the Internet and the cloud customers are sharing the computing resources. This help the cloud computing service providers to deliver a good quality computing services.

Cloud computing providers are offering different service models such as software as a service, platform as a service, and infrastructure as a service. The wide variety of cloud computing services have met the cloud customers' needs. On the other hand, it provides an open door for hackers to launch different types of attacks that targeted the cloud services.

There are many new information security risks that emerges with a cloud computing model [8]. These security risks must be investigated and evaluated. User's data privacy, data isolation, authorization and access control are examples of the security concerns when hosting many customers' data on the shared physical infrastructure as in the cloud computing environment [9].

The security perimeter has changed from a fixed boundary in the traditional computing to an elastic boundary that is constantly changing in the cloud computing; moreover, many threats are evolving, making it more difficult for the incident handler to analyze the information-system-based attack.

3. Cloud Computing Digital Forensic Challenges

There are many challenges that make the digital forensic investigations more complicated in a cloud computing environment. The distinguished characteristics of the cloud computing environment are the main reason for this complexity. This section discusses the most common digital forensic investigations challenges in a cloud computing environment such as volatile data issue, multi-tenancy issue, multi-jurisdiction issue, evidence in logs issue, time synchronization issue, Service Level Agreement (SLA), virtualization implementation issue, chain of custody issue, evidence correlation, data integrity, lack of forensics tools, data deletion issue, lack of standards, physical inaccessibility issue, ineffective encryption key management issue, large amounts of evidence size issues, difficult to conduct real time investigation in cloud and less control in cloud. Each issue will be briefly explained in order to get a better understanding of subject matter.

3.1. Volatile Data Issue

The nature of cloud storage usage is not permanent and the allocated storage will be erased and re-allocated to another customer as soon as the current customer subscription expire [10]. Not only the user's data will be removed, but also many important information within the virtual machine will be volatile when its restart or shutdown. This volatile data may include very important information for the digital investigations which may include registry entries and temporary internet files. In some case, cloud service providers automate this type of operations and their policies give short time before the storages of the expired customers' accounts is erased. This limitation in time will be one of the most popular challenges for the digital forensic investigators, where there is no sound information that investigators can based on to provide the required evidences. Thus, it is necessary that cloud computing service providers to develop an external repository for the logs of cloud system and the logs of the virtual machines.

3.2. Multi-Tenancy Issue

The digital forensic investigator's task is not only to extract the solid evidences from the victim data, but also to ensure other cloud customers' privacy and their data integrity. Protecting the cloud customers' privacy and their data integrity could be the main reason for the cloud service providers to not cooperate with digital forensic investigators. Besides, cloud service providers use multiple data centers to serve multi cloud computing customers may raise many uncertainties about customers' data isolating and retrieving [10].

3.3. Multi-Jurisdiction Issue

To avoid the loss of customers' data due to the natural disasters, cloud service providers locate their data centers in different geographical locations. Usually, these data centers located in different countries which for sure have different jurisdictions. This diversity of the laws is another challenge for the digital forensic investigations. Conducting a digital forensic investigation in such situation will require more international agreements and cooperation, which may not be ready yet in the case of a cloud computing environment [5]. This will add more efforts for the digital forensic investigators to customize their procedures to avoid local law violation.

3.4. Evidence in Log Files Issue

Every cloud service provider has their distinct cloud computing infrastructure that has its own structure of the different cloud computing models. Each cloud computing service model (such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS)) has different structure, contents, and formatting of the log files. This variety of the log files will be another challenge for the digital forensic investigators. Therefore, the digital forensic investigators need to understand and able to extract the required evidence from it [10].

3.5. Time Synchronization Issue

The differences of the time zones between servers of the cloud service provider and the devices of the cloud customers will lead to suspicions about the integrity and reliability of the collected data as evidence as mentioned in [11].

3.6. Service Level Agreement (SLA)

An SLA in a cloud computing environment is a contract between a cloud service provider and the cloud computing end user that defines the level of service expected from the service provider. It is essential that SLA supports the forensic investigations in a proper manner within specified time constraints. In [18-19] suggested some important points that should be addressed in the SLA as follows [12]:

- Tools, procedures, access and services that support forensics investigation.
- Forensics investigation roles and responsibilities of both cloud service provider and the cloud customer.
- Considering different jurisdiction laws and procedures.
- Availability of an incident response team.
- Formatting of the log files and operational records.

3.7. Chain of Custody Issue

In the traditional computing model, the standard practice in digital forensics investigations, the forensic investigators seize the suspected digital devices and conduct the required analyses with full access and control on the digital devices. Yet, in cloud computing model, taking custody on the suspected physical devices is not possible because the server that might contain the evidence is shared between multi-tenants. Usually, the digital forensics are granted only limited access to the server [13]. Based on the limited access to the abstracted resources, the forensic investigators must understand the cloud computing environment, including the cloud architecture, hardware, hypervisor and file system [14]. Thus, digital investigators in the cloud computing environment are facing many challenges because they have to work with minimum control in the cloud computing environment.

3.8. Evidence Correlation Issue

Most of the cloud computing customers depend on the mobile devices (such as notebook, smart phones) to access to the cloud services. In many cases, cloud customers use more than one device or maybe different devices as the data exist on the service provider data center and can be accessed from anywhere at any time. Besides, the fact that most of cloud computing providers have multiple data centers in different places. This will make the logs of data access and process distributed on different devices and locations, which consequently making it a difficult task on the digital forensic investigators to correlate all these devices and come out with solid and sound digital evidence [15].

3.9. Data Integrity Issue

Unlike traditional computing model, cloud computing model is still evolving which means there is a lack of good documentation and use of data integrity tools. Besides, the fact that cloud computing environment has heterogeneous nature will elevate doubts on the evidence integrity [14].

3.10. Lack of Forensics Tools

According to [10], there are many drawbacks for the traditional forensics tools to be used in the cloud computing environment. However, the current digital forensic tools are needed for large efforts of development and enhancement to fit for cloud computing environment.

3.11. Lack of Standards

Cloud computing model as the new and emerging model still suffers from lack of standardization. Most of the cloud service providers are using their own cloud computing structure. Therefore, cloud computing environment for each service provider may differ from one another [16]. This is another challenge for the digital forensic investigators to establish standard steps for cloud computing forensic investigations.

3.12. Larger Evidence Size Issue

Regional Computer Forensic Laboratory (RCFL) in their report published in 2012 stated that digital evidence size has been increased recently. In a comparison for digital evidence size that sized by RCFL in 2006 and 2013, they found out that it has been increased by 500%. This large size of the digital evidences needs for efficient and authentic digital forensic tools [10].

3.13. Difficult to Conduct Real Rime Investigation in Cloud

As result to demand self-service, resource pooling, multi-tenancy, and rapid elasticity characteristics of the cloud computing environment, the regular and even automated deleting of files from releasing storage has been used by the cloud service providers. In such environment, seizing and collecting digital evidence is a very difficult task for the forensic investigators. One of the solutions is by conducting real-time forensic investigations to collect the digital evidences in real-time. However, there are many challenges for live forensic investigation in the cloud computing environment. This kind of investigations need to be performed by intelligence processes with special legal means, most of the cloud service providers reject to authorize such processes because they do not want to reveal the details about their critical operations [17-18]. Moreover, the fact that the cloud computing model is a developing computing model makes the decision on the required processes for live forensic investigations a very difficult task [19].

4. Discussion

The cloud computing model has some distinct characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. On-demand self-service refers to the cloud customer’s ability to easily request cloud computing resources when he needs it and easily customize it with minimum interaction with the cloud service provider. Broad network access refers to the ability of the cloud customer to access to the cloud computing resources at anytime from anywhere. Rapid elasticity refers to the cloud customer’s ability to easily request extra computing resources when he needs it and easily release them back with minimum interaction with cloud service provider. Measured service refers to cloud computing customer’s ability to pay only for what he needs [6].

These characteristics differentiate the cloud computing model from the traditional computing models. The well-known security procedures and measurements in the traditional computing environment becomes inapplicable for the cloud computing environment. Digital forensic investigations are one of the important actions performed to find the necessary evidences in the digital crimes. However, conducting a digital forensic in the cloud computing environment is a hard task due to the challenges faced by the forensic investigators. In each process of the cloud computing digital forensic, there are different challenges that arise due to the cloud computing environment.

In the previous section, we discuss some of the challenges for cloud digital forensic investigations. In this section, we discuss the steps of cloud digital forensic investigation along with the different characteristics of cloud computing. Table 1 shows the expected challenges that will be faced in each step of digital forensic investigation due to the different cloud computing characteristics.

4.1. Identification

The first process of the digital forensic investigation is the identification process. During this process, the digital forensic investigator must determine the digital crime, any hardware or software used for committing the crime and the potential evidence [5]. The current forensic identification tools and techniques are not fit for cloud computing environment, because of the new characteristics of the cloud computing environment such as resources pooling, multi-tenancy, on demand self-service and rapid elasticity. The cloud computing environment is a distributed, shared and dynamic environment. Conducting an initial identification for the illegal activities in the cloud computing environment is almost impossible to be performed without relying on cloud service providers [14, 20].

The technologies used by the cloud service providers to offer cloud computing services with the guaranteed cloud computing characteristics may cause some challenges for the identification process during the cloud digital forensic investigation. As listed in Table 1, the expected challenges are as follows:

- On-demand self-service, resource pooling, and rapid elasticity: the virtualization techniques and system automation may cause some challenges such as volatile data, multi-tenancy, evidence in logs, service level agreement (SLA), real-time investigation and less control in the cloud.
- Broad network access: unsafe usage such as the use of Internet to access to the cloud resources may cause some challenges such as multi-jurisdiction, evidence in logs, service level agreement (SLA), real-time investigation and less control in the cloud.
- Measured Service: using online systems, user’s usage monitoring tools and automated systems may cause some challenges such as multi-tenancy, multi-jurisdiction, evidence in logs, service level agreement (SLA), real-time investigation and less control in the cloud.

Table 1: Cloud Computing Characteristics and Digital Forensic Steps.

		Cloud Computing Characteristics				
		On-demand self-service	Broad network access	Resource pooling	Rapid elasticity	Measured Service
Forensic Steps	Identification	• Volatile Data • Multi-tenancy • Evidence in logs • Service Level Agreement (SLA) • Real-Time Investigation • Less Control in Cloud	• Multi-jurisdiction • Evidence in logs • Service Level Agreement (SLA) • Real-Time Investigation • Less Control in Cloud	• Volatile Data • Multi-tenancy • Evidence in logs • Service Level Agreement (SLA) • Real-Time Investigation • Less Control in Cloud	• Volatile Data • Multi-tenancy • Evidence in logs • Service Level Agreement (SLA) • Real-Time Investigation • Less Control in Cloud	• Multi-tenancy • Multi-jurisdiction • Evidence in logs • Service Level Agreement (SLA) • Real-Time Investigation • Less Control in Cloud
	Data Collection and Preservation	• Volatile Data • Multi-tenancy • Multi-jurisdiction • Evidence in logs • Time Synchronization • Service Level Agreement (SLA) • Virtualization • Chain of Custody • Data Integrity • Data Deletion • Lack of Standards • Physical Inaccessibility • Real-Time Investigation • Less Control in Cloud	• Multi-jurisdiction • Evidence in logs • Time Synchronization • Service Level Agreement (SLA) • Chain of Custody • Data Integrity • Lack of Standards • Physical Inaccessibility • Real-Time Investigation • Less Control in Cloud	• Volatile Data • Multi-tenancy • Multi-jurisdiction • Evidence in logs • Time Synchronization • Service Level Agreement (SLA) • Virtualization • Chain of Custody • Data Integrity • Data Deletion • Lack of Standards • Physical Inaccessibility • Real-Time Investigation • Less Control in Cloud	• Volatile Data • Multi-tenancy • Multi-jurisdiction • Evidence in logs • Time Synchronization • Service Level Agreement (SLA) • Virtualization • Chain of Custody • Data Integrity • Data Deletion • Lack of Standards • Physical Inaccessibility • Real-Time Investigation • Less Control in Cloud	• Multi-tenancy • Multi-jurisdiction • Evidence in logs • Time Synchronization • Service Level Agreement (SLA) • Chain of Custody • Data Integrity • Lack of Standards • Physical Inaccessibility
	Analysis & Examination	• Evidence in logs • Time Synchronization • Evidence Correlation • Lack of Forensics Tools • Encryption • Evidence size	• Evidence in logs • Time Synchronization • Evidence Correlation • Lack of Forensics Tools • Encryption • Evidence size	• Evidence in logs • Time Synchronization • Evidence Correlation • Lack of Forensics Tools • Encryption • Evidence size	• Evidence in logs • Time Synchronization • Evidence Correlation • Lack of Forensics Tools • Encryption • Evidence size	• Evidence in logs • Time Synchronization • Evidence Correlation • Lack of Forensics Tools • Encryption • Evidence size
	Presenta	• Virtualization • Chain of Custody	• Virtualization • Chain of Custody	• Virtualization • Chain of Custody	• Virtualization • Chain of Custody	• Virtualization • Chain of Custody

4.2. Data Collection and Preservation

The second process of the digital forensics is data collection and preservation. During this process, the digital forensic investigator must preserve the suspected physical digital device to ensure that evidence integrity is not violated. To maintain the evidence integrity, the investigator must extract the exact bit-by-bit image of the required data. In addition, the use of hash functions is considered as the best practice to verify the integrity of the extracted image [5].

However, in a cloud computing environment, preserving the physical device is not possible. The physical device in a cloud computing environment is owned by the cloud service provider and shared between multi-tenants. Besides, the physical devices might exist in different geographic locations. Moreover, cloud service providers depend on the virtualization techniques to build the cloud environment. In such environment, the user's data will be removed when the user releases the resource that he used, adding another challenge for the cloud forensic investigators.

The cloud computing model has different service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The responsibility and authorities of cloud customer and cloud service provider are changed in each service model. Therefore, the cloud forensic investigator must understand the structure of each model to be able to determine where he should be looking for the digital evidence.

The technologies used by the cloud service providers to offer cloud computing services with the cloud computing characteristics may cause some challenges for the data collection and preservation process during the cloud digital forensic investigation. As listed in Table 1, the expected challenges are as follows:

- On-demand self-service, resource pooling, and rapid elasticity: The virtualization techniques and system automation may cause some challenges such as volatile data, multi-tenancy, multi-jurisdiction, evidence in logs, time synchronization, service level agreement (SLA), virtualization, chain of custody, data integrity, data deletion, lack of standards, physical inaccessibility, real-time investigation and less control in the cloud.
- Broad network access: Unsafe usage, such as using the Internet to access to the cloud resources may cause some challenges such as multi-jurisdiction, evidence in logs, time synchronization, service level agreement (SLA), chain of custody, data integrity, lack of standards, physical inaccessibility, real-time investigation and less control in the cloud.
- Measured Service: Using online systems, user's usage monitoring tools, and automated systems may cause some challenges such as multi-tenancy, multi-jurisdiction, evidence in logs, time synchronization, service level agreement (SLA), chain of custody, data integrity, lack of standards and physical inaccessibility.

4.3. Analysis and Examination

The most important process of the digital forensics is analysis process. In this process, the collected digital data is examined and analysed to find the evidence that a suspected person has committed a crime. Unlike the digital forensics in the traditional computing environment, where the structure of the environment is well known, the structure of the cloud computing environment is different from service provider to another. Besides, the data formats in cloud computing environment are different for each cloud service model [14]. The digital forensic examining tools used in the traditional computing environment will be limited and useless in the cloud computing environment.

The technologies used by cloud service providers to offer cloud computing services with the cloud computing characteristics may cause some challenges for the analysis and examination process during the cloud digital forensic investigation. The virtualization techniques, system automation, and serving multi customers may cause some challenges such as evidence in logs, time synchronization, evidence correlation, lack of forensic tools, encryption and evidence size.

4.4. Presentation

The last process of the digital forensics is presenting the findings of the evidence analysis in court. Presenting the findings of the forensic analysis might include crime scene reconstruction, which might be easy in the traditional computing environment, but very difficult in the cloud computing environment. The technologies used by the cloud service providers to offer cloud computing services may cause some challenges for the presentation process during the cloud digital forensic investigation. The virtualization techniques and multiple data centers may cause some challenges such as virtualization and chain of custody.

5. Conclusion

The unique features of the cloud computing model have brought many great advantages for the both the individual users and organizations, yet, on the other hand rise many security concerns and difficulties. However, the security issues must be addressed and evaluated carefully before migrating to the cloud computing environment. Therefore, in this paper, we discussed some of the challenges faced by the digital forensic investigators in cloud computing environment. Thus, our future work will be proposing an appropriate digital forensic approach for cloud computing.

Acknowledgement

The authors would like to thank Universiti Teknologi Malaysia (UTM) and Ministry of Higher Education, Malaysia for their assistance and support for this work through the Fundamental Research Grant Scheme (FRGS) under vote number RK130000.7838.4F714.

References

[1] Doherty, E., Carcary, M., & Conway, G. (2015). Migrating to the cloud: Examining the drivers and barriers to adoption of cloud computing by SMEs in Ireland: An exploratory study. Journal of Small Business and Enterprise Development, 22(3), 512-527.

[2] Tabona, O., & Blyth, A. (2016). A forensic cloud environment to address the big data challenge in digital forensics. Proceedings of the SAI Computing Conference, pp. 579-584.

[3] Yin, L. (2012). Study on computer forensics in cloud computing. Proceedings of the IEEE International Conference on Computer Science & Service System, pp. 1717-1719.

[4] NIST Cloud Computing Forensic Science Working Group. (2014). NIST cloud computing forensic science challenges (Draft). NIST Interagency Report 8006.

[5] Almulla, S. A., Iraqi, Y., & Jones, A. (2014). A state-of-the-art review of cloud forensics. Journal of Digital Forensics, Security and Law, 9(4), 7-28.

[6] International Organization for Standardization (ISO). (2014). ISO/IEC 17788:2014 Information technology - Cloud computing - Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en.

[7] Skene, J., Raimondi, F., & Emmerich, W. (2010). Service-level agreements for electronic services. IEEE Transactions on Software Engineering, 36(2), 288-304.

[8] Alsubaih, A., Hafez, A., & Alghathbar, K. (2013). Authorization as a service in cloud environments. Proceedings of the IEEE Third International Conference on Cloud and Green Computing, pp. 487-493.

[9] Yang, C. N., & Lai, J. B. (2013). Protecting data privacy and security for cloud computing based on secret sharing. Proceedings of the IEEE International Symposium on Biometrics and Security Technologies, pp. 259-266.

[10] Samy, G. N., Shanmugam, B., Maarop, N., Magalingam, P., Perumal, S., & Albakri, S. H. (2017). Digital forensic challenges in the cloud computing environment. Proceedings of the International Conference of Reliable Information and Communication Technology, pp. 669-676.

[11] Zawoad, S., & Hasan, R. (2013). Digital forensics in the cloud. http://www.dtic.mil/dtic/tr/fulltext/u2/a590911.pdf.

[12] Barrett, D., & Kipper, G. (2010). Virtualization and forensics: A digital forensic investigator's guide to virtual environments. Syngress.

[13] Alex, M. E., & Kishore, R. (2016). Forensic model for cloud computing: an overview. Proceedings of the IEEE International Conference on Wireless Communications, Signal Processing and Networking, pp. 1291-1295.

[14] Alqahtany, S., Clarke, N., Furnell, S., & Reich, C. (2015). Cloud forensics: a review of challenges, solutions and open problems. Proceedings of the IEEE International Conference on Cloud Computing, pp. 1-9.

[15] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7, S64-S73.

[16] Albakri, S. H., Shanmugam, B., Samy, G. N., Idris, N. B., & Ahmed, A. (2014). Security risk assessment framework for cloud computing environments. Security and Communication Networks, 7(11), 2114-2124.

[17] Decker, M. J., Kruse, W., Long, B., & Kelly, G. (2011). Dispelling common myths of live digital forensics. http://dfcb.org/wp-content/uploads/2018/05/myth-of-live-forensics.pdf.

[18] Ruan, K. (2013). Cybercrime and cloud forensics: Applications for investigation. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.394.7732&rep=rep1&type=pdf.

[19] Ruan, K., & Carthy, J. (2012). Cloud forensic maturity model. Proceedings of the International Conference on Digital Forensics and Cyber Crime, pp. 22-41.

[20] Pătraşcu, A., & Patriciu, V. V. (2013). Beyond digital forensics. A cloud computing perspective over incident response and reporting. Proceedings of the IEEE 8th International Symposium on Applied Computational Intelligence and Informatics, pp. 455-460.