A Comprehensive Study of Current and Future Trends in Cloud Forensics

Sandesh Achar

Director of Cloud Engineering, Workday Inc., Pleasanton, California, USA

ISSN: 2311-8636 (Print)
ISSN: 2312-2021 (Online)

Source of Support: Nil

No Conflict of Interest: Declared

***Email for correspondence:**
sandeshachar26@gmail.com

ABSTRACT

Organizations are increasingly turning to cloud computing, which offers convenience and provides services based on virtualization technology. Some benefits of cloud computing include accessibility, availability, flexibility, vast storage capacity, speed, flexibility, and on-demand network connectivity. Significant potential security dangers are associated with this new technology, and digital forensics cannot keep up with the rapid adoption of cloud computing solutions. This study gives an overview of cloud forensics to offer better prospects, highlighting the existing problems and difficulties. It also suggests actions that can be taken to address these difficulties.

Keywords: Cloud Computing, Digital Forensics, Technology Virtualization, Storage Capacity

INTRODUCTION

Cloud computing is one of the leading technologies making IT infrastructure available to institutions and companies in new ways by delivering storage services through virtualization-based technologies. Cloud computing technologies offer improved speed, huge storage capacity, greater availability, scalability, on-demand network access, and convenience to a joint pool of accessible computing resources while reducing costs (Achar, 2021b). Lately, it has been realized that cloud computing provides the best services ranging from business applications to fast access, drastically boosting infrastructure resources. However, some concerns have been raised regarding compliance integrity and security. Cloud computing provides significant economic benefits to users by offering scalable infrastructure such as pay-as-you-use services, lower energy consumption, and on-demand computing. However, this technology poses several threats, such as criminal manipulation with little evidence and allowing easy access to other malicious activities. The two main concerns for adopting the cloud are privacy and security. Due to these concerns, several institutions and sectors are cautious about implementing cloud computing. Several techniques are being incorporated within cloud computing platforms to address these concerns to ensure general security requirements are met for full cloud deployment.

CLOUD FORENSICS

Cloud forensics is a branch of computer security that addresses incidents using cloud infrastructure. Even though cloud computing is primarily an online technology, the incident under investigation need not have occurred online (Manral et al., 2020). However, the structural complexity of the cloud (a collection of different technologies, such as resource virtualization, utility computing, and distributed systems) is one reason cloud forensics is more complex than conventional computing devices and mobile application forensics. Several issues have been raised, such as the incompatibility and unreliability of current tools and mechanisms to support cloud forensic investigations. Sources of evidence can be client-based, server-based, or network-based (Achar, 2020a). Some of the research studies have been on client-based forensic analysis, somewhat because it is difficult, if not impractical, for researchers to perform forensic analysis on commercial cloud servers, such as those belonging to Google and Amazon.

There is a growing emphasis on cloud forensics owing to the extensive usage of cloud facilities and the current context of confidentiality consciousness, such as the promulgation of the General Data Protection Regulation. The capacity of an investigator to quickly locate and gather pertinent items of evidence may need to be improved by several circumstances, such as the difficulty in determining the exact physical position of the hardware resources, virtualization, and distributed environments. Another element that could obstruct an inquiry is jurisdiction, as the investigator could lack jurisdiction over data held in a foreign country.

STEPS INVOLVED IN CLOUD FORENSICS

Cloud forensics can be implemented using the steps highlighted in Figure 1.

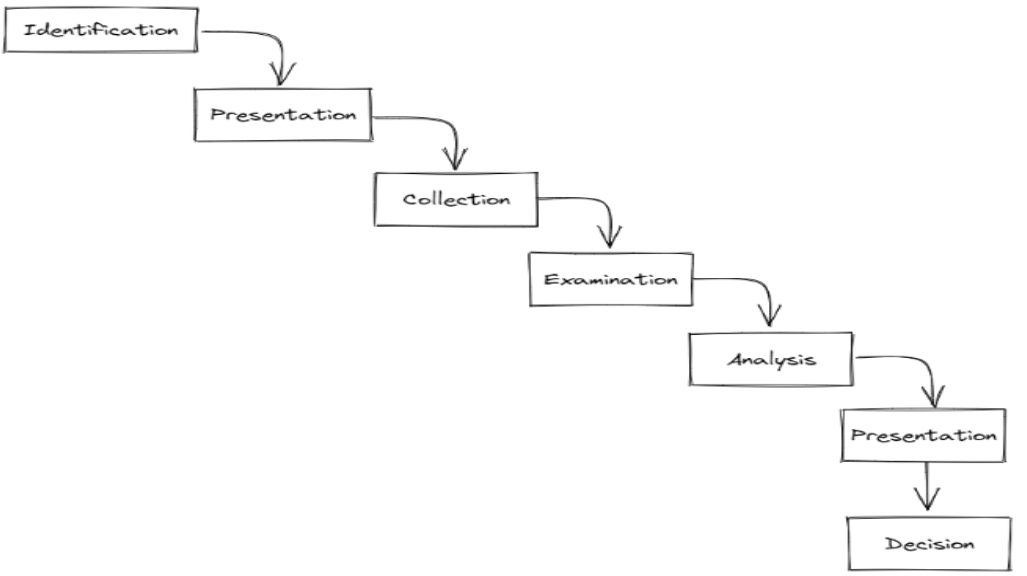

Figure 1: Steps Involved in Cloud Forensics.

- Identification: Before beginning a forensic investigation, one must ascertain whether any wrongdoing occurred. Once this has been confirmed and identified, the investigator can begin their inquiry.
- Preservation: The information gathered throughout the investigation is crucial to the investigation process and should be stored for future use.

- Collection: Whatever evidence was gathered throughout the investigation should be appropriately preserved.
- Examination: All the information gathered throughout the forensic inquiry in the cloud must be thoroughly scrutinized to conclude.
- Analysis: For the investigator to conclude what might have been done with the data by the intrusive party, the acquired and inspected data must be correctly assessed.
- Presentation: The presentation is critical because the information gathered is technical data that must be presented in the cyber court. In addition, some judges need help understanding the technical vocabulary.
- Decision: This is the final stage, during which the investigator and organization decide what to do with the situation analysis results.

CLOUD FORENSICS SOLUTION NOMENCLATURE

Existing cloud forensic studies can be divided into four categories, as illustrated in the subsection below. The categories focus on the different resources and actors in the cloud, except the first category, which focuses on security events. Every investigation begins with a specific incident. Models, systems, frameworks, and solutions for the security incident that initiates the forensic inquiry might contribute to cloud forensics.

Incident-driven Cloud Forensics

Security incidents, such as violations of security procedures and the application or enforcement of those policies, are increasingly common in today's IT-driven economy (Achar, 2020a). Security events typically catalyze a digital inquiry, serving as the first category's foundation. We further divided the forensic examination of incidents into two categories in our classification: pre- and post-incident forensics. Pre-incident forensics are viewed as continuous in this study and are sometimes referred to as "forensic preparation" in the literature. A condensed depiction of incident-driven forensics is shown in Figure 2. The figure's first section, on the right, shows an illustration of ongoing forensics through centralized logging, whereas the second section shows a post-incident review (left). Logs are viewed as forensic artifacts in both chambers of the investigation.

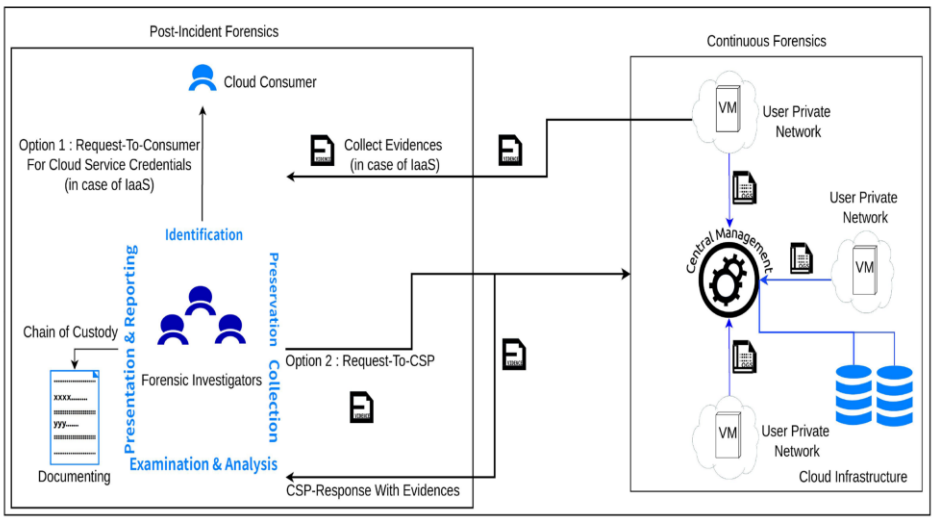

Figure 2: Incident-driven cloud forensics (Manral et al., 2020) contains central logging

techniques for ongoing forensics. In the second subcategory (post-incident forensics), there are two ways to obtain artifacts: (1) using cloud consumer credentials and (2) by contacting the cloud service provider.

Provider-driven Cloud Forensic

Cloud service providers (CSPs) play a critical role in forensic investigations, especially when they host and manage the underlying physical infrastructure where customers' applications and data are stored. Service models are crucial to forensics because they impact how much control employees have over their workplace. In addition, agent-based and log-based CSP-dependent methods are examined in Tables 1 and 2.

Table 1: Overview of Log-based Solutions

Log-based Solutions
Trenwith et al. (2013) anticipated a central logging model for cloud forensics preparedness.
Patrascu & Patriciu (2015) presented cloud forensic components that collect forensic and log data from virtual machines as a logging framework for cloud architecture with forensic support.
Kebande & Venter (2015) presented an efficient architecture using MapReduce for quick and effective digital exploration.
Rane & Dixit (2019) proposed a secure logging-as-a-service (BlockSLaaS) for the cloud environment based on blockchain technology.
Wang et al. (2019) proposed a public auditing paradigm for outside auditors to verify the accuracy of cloud storage logs.
Kumar Raju & Geethakumari (2018) proposed an outline and a system for event reconstruction in a cloud domain.

In addition, Manral et al. (2019) deduced that provider-driven solutions strongly emphasize ongoing, centralized evidence collection and forensic readiness for the fundamental cloud infrastructure. Most techniques in this category emphasize the continual evaluation CSPs conduct as a service for consumers and investigators.

Table 2: Overview of Agent-based Solutions

Agent-based Solutions
Kebande & Venter (2016) discussed the agent-based solution service, which collects data from virtual machines and makes it available to investigators as evidence. Hashing was used to guarantee the integrity of the evidence as well (ABSaaS).
Kebande & Venter (2014) proposed using bots as nonstop forensic agents in the cloud and put the notion into practice with botnet-as-a-service SaaS (BaaS).
Lu et al. (2010) added a forensic agent on the VM to collect the essential data and transfer it to the forensic center for archiving and further analysis.

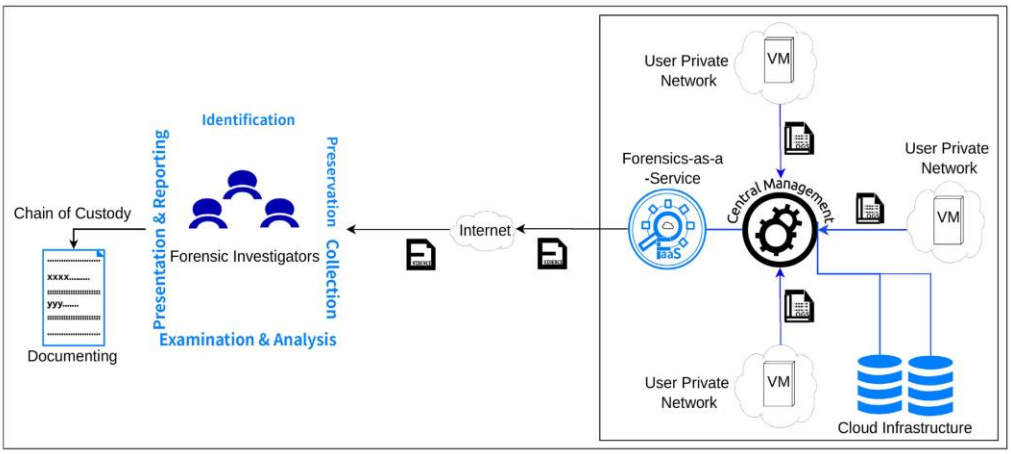

Figure 3: Provider-driven cloud forensics (Manral et al., 2020)

Consumer-driven Cloud Forensics

As was stated earlier, it is widely understood that CSPs are essential to cloud forensics. Put another way; forensic investigators must work with CSPs to gather evidence because they have less prominence and grip over the cloud architecture, particularly in PaaS and SaaS environments. There are also various operational and legal difficulties therein. Even if the CSP cooperates, evidentiary reliability, integrity, and chain of custody must be considered. Therefore, consumer-driven solutions that take trust into account are needed. Figure 4 illustrates a consumer-driven forensic system using a forensic server, which serves as a central repository for evidence.

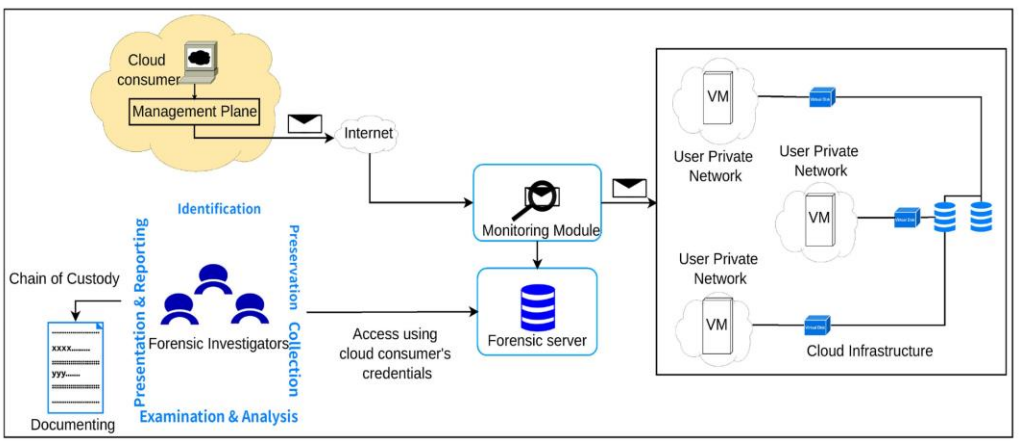

Figure 4: Consumer-driven Cloud Forensics (Manral et al., 2020): Demonstrating Two Independent Solutions of Cloud Service Providers.

Resource-driven Cloud Forensics

Cloud computing is a business-oriented pay-as-you-go paradigm, which resources as services to customers; it is also used for resource metering and utility computing (Achar, 2020b). Virtualization in the cloud extends beyond network virtualization; servers and storage are generally regarded as the essential elements of a cloud system. However,

virtualization provides for greater hardware utilization in the cloud, but it brings new challenges to forensics: the cloud's gain is forensics' loss. The characteristics of a cloud include multi-tenancy, data dispersion, and redundancy; however, these characteristics provide difficulties for forensics. Most CSPs offer the three essential services of computing, storage, and networking. In the cloud, these terms refer to virtual disks and virtual networks instead of the bare physical hardware in virtual machines with CPUs. The resource-driven forensics is shown in Figure 5, which can be divided into three components: Software-defined Networking forensics, Storage forensics using client-side artifacts, and VM forensics, which includes virtual machine isolation, and virtual machine snapshots.

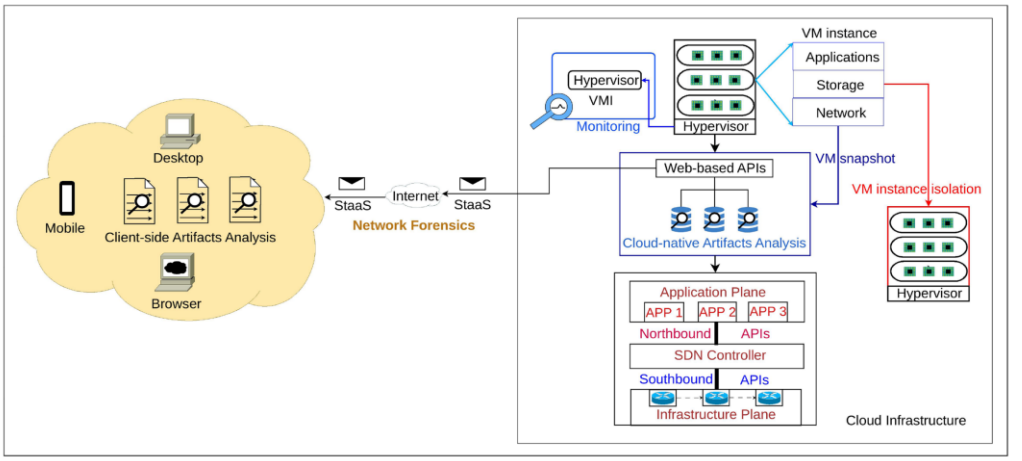

Figure 5: Resource-driven Cloud Forensics (Manral et al., 2020): The solution includes potential forensic sites in SDN architecture, client and server-side artifact analysis, virtual machine instance separation, VM snapshots, and VMI.

CURRENT TRENDS

The nature of emerging technologies and the growing number of devices implementing them make it necessary to develop digital forensic tools as a continuous activity. In addition, numerous digital forensics tools and their features are listed in a catalog of the NIST's features.

Traditional Digital Forensic Tools

An open-source platform for forensic investigations that includes identifying, gathering, and preserving evidentiary artifacts is called the Digital Forensic Framework (DFF). Due to its compatibility with VMware (VMDK) and support for VM disk reconstruction, DFF expands its capability to the virtual environment. Network packet capturing, protocol investigation, traffic sifting, and visualization tools include Wireshark, Wildpackets Omnipeek Enterprise, and Network Miner. File and folder recovery, file signature analysis, hash analysis, location of email and Internet artifacts, and data and metadata indexing are the significant features of such forensic solutions. A forensic toolbox involves grouping forensic tools in one location. It can include OCR, file decipherment, data modeling, malware triage, email analysis, and data visualization.

A complete set of investigative tools for conducting digital inquiries is available in the AccessData Forensic ToolKit (FTK). These technologies have been used extensively in forensic investigations for cloud environments. For example, enCase and FTK were assessed

by Dykstra and Sherman (2012) for their suitability in the cloud context for remote acquisition. FTK was also used by Alex and Kishore (2017) to record, archive, and examine forensic photos that comprised network traffic and VM status.

Cloud-specific Tools

Due to its design and isolated characteristics, forensic examiners face additional obstacles while using the cloud. Regarding the cloud, compatibility and dependability are the fundamental problems with traditional Digital Forensic (DF) tools. FROST is an API-based forensic tool for the OpenStack cloud environment (Dykstra and Sherman, 2012). It supports the IaaS service paradigm and comprises three API-based means for the reliable forensic procurement of guest firewall logs, API logs, and virtual disks. The fundamental restriction of the FROST tool is faith in the CSP because it necessitates trust in components owned by the CSP, such as the hypervisor, hardware, and networking infrastructure underneath the guest operating system. To address the limitations of the client-based analysis, such as limited data replication and revision recovery concerning cloud storage, a service provider has developed an API-based forensic tool called Kumodd to examine cloud-side artifacts. An analysis tool for Google Docs called Kumodocs is based on the DraftBack browser add-on.

OPPORTUNITIES AND CHALLENGES FOR CLOUD FORENSICS

The study of Ruan et al. (2013) explained some opportunities and challenges faced by digital forensics investigations in cloud environments. Figure 6 presents opportunities and findings of cloud forensics. Solid procedures and robust tools must be employed in digital forensics. The following section highlights the impacts of digital forensics on cloud computing.

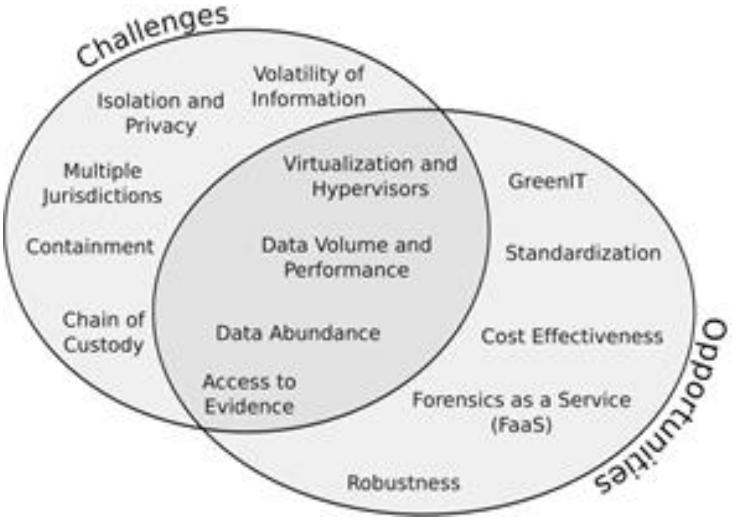

Figure 6: Challenges and Opportunities of Cloud Forensic (Poisel & Tjoa, 2012).

- Complexity: Vatsenko (2020) reported that cloud forensics often involves multi-dimensional levels of intricacy. For example, hypervisor vendors offer their customers various application programming interfaces with a limited life cycle. Each hypervisor structure impacts the architecture of occurrences running in the cloud. In addition, the exchange of information between cloud service providers may further complicate the forensic examination of such systems.

- Privacy Isolation: Cloud providers offer multi-tenant storage to their customers, and it is believed that storage can become infected through customers' access to the storage units. Thus, data forensics must be acquired before investigations. Another issue is that availability problems can result from isolation from all other related instances.
- Standardization: Technology change always brings about new standards to accommodate the newly implemented technology. However, due to the early stage, it is possible that standardized measures for cloud forensics progress together with the growth of cloud computing as it evolves.
- Hypervisors and Virtualization: Virtualization is a common foundation for cloud deployments, with CSPs implementing cloud computing instances in virtualized environments. Hypervisors keep track of and provision running cases. The hypervisor is the fundamental component in cloud architecture, and any successful attack could jeopardize the security of all systems under its control. In addition, there are methods for malware detection and removal in virtual environments. Still, there are no policies, practices, or procedures at the hypervisor level to help with digital forensics investigations. By enabling the correlation of data gathered from various hypervisors, future tools for examining cloud infrastructures will further solve this issue.
- Chain of Custody: Documenting the chain of custody in cloud computing is now a problem that must be solved. The data stored in the cloud can be accessed logically only using service models like SaaS. In online circumstances, conventional approaches (such as computing hash values) that demonstrate data integrity may be useless. Organizational frameworks are made up of best practices and procedures. They outline the precautions to take for digital forensics investigations (Poisel & Tjoa, 2012). Implementing an organizational framework suited explicitly for digital forensics in Cloud computing is necessary to solve the chain of custody issues.
- Cost Effectiveness: It is possible to plan and use the computer power needed for digital forensics investigations with forensics-as-a-service (FaaS).
- GreenIT: Due to the lack of natural resources available for energy generation, developments are vital to optimize and power IT infrastructures and modern electronics' energy usage. For example, FaaS may utilize unused computing resources, meeting the criteria for Green IT.

FUTURE DIRECTIONS

Investigators working in a cloud setting must use all cloud service models to examine a sizable amount of evidence that has been gathered. One such free and open-source cloud computing software platform is called OpenStack. Users typically use it as an IaaS. When log data are kept in the hash table, nontrivial issues in accumulating remote evidence are overcome, making this method less dependent on CSPs than standard acquisition techniques. However, in the case of SaaS and PaaS, where consumers have less influence over the proposed cloud infrastructure, investigators are typically more dependent on CSPs. Different CSPs provide customer services in the cloud architecture according to their needs.

Given that the cloud is a distributed platform, users should be able to choose from various CSPs rather than a single provider when purchasing cloud services. Every CSP is located within a network or sub-networks. In this regard, all those hosts that are inter- and intra-related must be considered during the investigation procedure when malicious behavior is reported. Customers will only give complete cloud control over computation if CSPs can guarantee the integrity of the information. The cloud forensics investigators' perspective is also a key point of emphasis here. For example, a job-based SaaS cloud model with an

integrity verification mechanism was suggested elsewhere in consideration of this. There is always a concern about evidence integration verification effectively and accurately because of the heavy reliance on CSPs, as investigators must gather all the evidence from a dispersed cloud architecture (Achar, 2021a). Future research should focus on creating a reliable and practical framework for the investigator to be aware of throughout the gathering and integrating evidence.

CONCLUSION

Internet and cloud computing are related in many ways, making them increasingly susceptible to security threats from all platforms deployed. Digital forensic experts must extend their expertise and toolset to carry out cloud examinations. Additionally, cloud service providers, cloud-based entities, and cloud service customers must consider incorporating built-in forensic functionalities. This paper highlights the previous and existing trends in cloud forensics. Cloud forensics requires a separate dedicated framework to ensure that investigators can customize it to meet their needs. For investigators working with cloud forensic principles, there is a significant expertise demand. In addition, common laws should be imposed without creating obstacles concerning jurisdictions. Much work needs to be done concerning cyber laws since cloud-based crimes can be adjudicated by legal persons who may or may need to gain sound technical knowledge.

REFERENCES

Achar, S. (2020a). Cloud and HPC Headway for Next-Generation Management of Projects and Technologies. Asian Business Review, 10(3), 187-192. https://doi.org/10.18034/abr.v10i3.637

Achar, S. (2020b). Influence of IoT Technology on Environmental Monitoring. Asia Pacific Journal of Energy and Environment, 7(2), 87-92. https://doi.org/10.18034/apjee.v7i2.649

Achar, S. (2021a). An Overview of Environmental Scalability and Security in Hybrid Cloud Infrastructure Designs. *Asia Pacific Journal of Energy and Environment*, *8*(2), 39-46. https://doi.org/10.18034/apjee.v8i2.650

Achar, S. (2021b). Enterprise SaaS Workloads on New-Generation Infrastructure-as-Code (IaC) on Multi-Cloud Platforms. *Global Disclosure of Economics and Business*, *10*(2), 55-74. https://doi.org/10.18034/gdeb.v10i2.652

Alex, M. E. & Kishore, R. (2017). Forensics framework for cloud computing. *Computers & Electrical Engineering, 60*, 193-205. https://doi.org/10.1016/j.compeleceng.2017.02.006

Dykstra, J. & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation,* S90—S98. https://doi.org/10.1016/j.diin.2012.05.001

Kebande, V. & Venter, H. S. (2015). A functional architecture for cloud forensic readiness large-scale potential digital evidence analysis. In Proceedings of the European Conference on Cyber Warfare and Security. Academic Conferences Int'l Limited, 373.

Kebande, V. R. & Venter, H. S. (2016). On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges. *Australian Journal of Forensic Sciences. 50*(2), 209-238. https://doi.org/10.1080/00450618.2016.1194473

Kebande, V. R. & Venter, H. S. (2014). A cognitive approach for botnet detection using Artificial Immune System in the Cloud. In: 2014 Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). Beirut, Lebanon. IEEE. https://doi.org/10.1109/cybersec.2014.6913971

Kumar Raju, B. K. S. P. & Geethakumari, G. (2018). Advances in Intelligent Systems and Computing. Singapore: Springer Singapore. Timeline-Based Cloud Event Reconstruction Framework for Virtual Machine Artifacts, 31-42. https://doi.org/10.1007/978-981-10-3376-6_4

Lu, R., Lin, X., Liang, X., and Shen, X. S. (2010). Secure provenance: The essential of bread and butter of data forensics in cloud computing. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 282–292.

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. https://doi.org/10.1145/3361216

Manral, B., Somani, G., Choo, K-K. R., Conti, M., and Gaur, M. S. (2020). A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions. *ACM Computing Surveys, 52*(6), Article 124. https://doi.org/10.1145/3361216

Patrascu, A., Patriciu, V-V. (2015). Logging for Cloud Computing Forensic Systems. *International Journal of Computers Communications & Control, 10*(2). https://doi.org/10.15837/ijccc.2015.2.802

Poisel, R., Tjoa, S. (2012). Discussion on the Challenges and Opportunities of Cloud Forensics. In: Quirchmayr, G., Basl, J., You, I., Xu, L., Weippl, E. (eds) Multidisciplinary Research and Practice for Information Systems. CD-ARES 2012. *Lecture Notes in Computer Science, 7465*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-32498-7_45

Rane, S. & Dixit, A. (2019). Communications in Computer and Information Science. Singapore: Springer Singapore. BlockSLaaS: Blockchain Assisted Secure Logging-as-a-Service for Cloud Forensics; p. 77-88. https://doi.org/10.1007/978-981-13-7561-3_6

Ruan, K., Carthy, J., Kechadi, T., Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results, *Digital Investigation, 10*(1), 34-43. https://doi.org/10.1016/j.diin.2013.02.004

Trenwith, P. M., & Venter, H. S. (2013). *Digital forensic readiness in the cloud.* In: 2013 Information Security for South Africa; 2013 Aug 14-16; Johannesburg, South Africa. IEEE. https://doi.org/10.1109/issa.2013.6641055

Vatsenko, A. (2020). Digital Forensics Techniques Overview. *Bulletin of Science and Practice, 6*(6), 167-174. https://doi.org/10.33619/2414-2948/55/21

Wang, J., Peng, F., Tian, H., Chen, W., Lu, J. (2019). Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Cham: Springer International Publishing. Public Auditing of Log Integrity for Cloud Storage Systems via Blockchain, 378-387. https://doi.org/10.1007/978-3-030-21373-2_29

--0--