The ISC Int'l Journal of Information Security

November 2021, Volume 13, Number 3 (pp. 49–57)

http://www.isecure-journal.org

Selected Paper at the ICCMIT'21 in Athens, Greece

Forensic-Enabled Security as a Service (FESaaS) - A Readiness Framework for Cloud Forensics **

Wedad Alawad [1,*], and Awatef Balobaid [2]

[1] *Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia.*
[2] *College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia.*

ARTICLE INFO.

Keywords:
Cloud Computing, Digital Forensic, Cloud Forensic, Cloud Security

Type: Research Article

doi:
10.22042/ISECURE.2021.0.0.0

dor: 20.1001.1.20082045.2021.13.3.6.3

ABSTRACT

Digital forensics is a process of uncovering and exploring evidence from digital content. A growth in digital data in recent years has made it challenging for forensic investigators to uncover useful information. Moreover, the applied use of cloud computing has increased significantly in the past few years and has introduced new challenges to forensic experts. Cloud forensics assists organizations that exercise due diligence and comply with the requirements related to sensitive information protection, maintain the records required for audits and notify concerned parties when confidential information is compromised or exposed. One of the problems with cloud forensics is the limitation of cloud forensic models and guidelines. This project aims to propose a new cloud forensic model that will help investigators and cloud service providers achieve digital forensic readiness within the cloud environment. To achieve this goal, we have studied and compared different forensic process models to determine their limitations. Based on the results of this comparative study, a new cloud forensic framework– Forensic-enabled Security as a Service (FESaaS) is presented. The security and forensic layers are aggregated to discover evidence in the proposed framework. Compared to other cloud forensic frameworks, our framework deals with live data, reports, and logs. Thus, it is sufficient and provides the capability for rapid response.

1 Introduction

Cloud forensics can be referred to as the cross-discipline of digital forensics and cloud computing. Cloud computing is generally a shared collection of network resources that are configurable for example servers, networks, applications, services, and storage which can be easily and quickly reconfigured without much effort. Digital forensics, on the other hand, can be thought of as the application of principles of computer science for recovering electronic evidence that can be presented in a court of law [1, 2]. The subset of forensics of networks is called cloud forensics. Digital forensics is used for investigations related

* Corresponding author.
**The ICCMIT'21 program committee effort is highly acknowledged for reviewing this paper.
Email addresses: wmaoad@qu.edu.sa, asbalobaid@jazanu.edu.sa
ISSN: 2008-2045

to networks. Therefore, cloud forensics deals with the main phases of digital forensics combined with techniques made for cloud environments.

Cloud computing is an emerging technology with complex aspects. It has also reduced the cost of IT, contributing to its fast adoption by government and business. To ensure the availability of service, cloud-based data centers are managed by CSPs (Cloud Service Providers) all around the world. The data stored at any of the data centers is being replicated at several locations to reduce the failure risk and abundance. Furthermore, there is a segregation of tasks performed between customers and CSP with respect to the responsibilities of forensics, which differs per the use of service models [2].

Multi-tenancy and multiple jurisdictions are creating additional challenges related to legal aspects. Most cloud forensics requires interaction between the customers and CSPs, the multiple tenants sharing resources, as well as international law enforcement agencies. To achieve more comprehensive analyses in the cloud forensic domain, legal, organizational, and technical dimensions of cloud forensics are used [3], [4], [5].

This study presents a cloud forensics framework "Forensic-enabled Security as a Service (FESaaS)". In this framework, several cloud resources will be used to acquire evidence from the cloud environment. FESaaS uses accessible information in building a case before executing a costly data acquisition process. Most cloud service providers offer security as a service. Thus, we also assert that digital forensic services can be offered as a service to achieve digital forensic readiness within the cloud environment. In our proposed framework, the Security as a Service will be Forensic Enabled. It can either be built-in within the cloud services or implemented by a third party that has used an interaction between the cloud services and the clients. The proposed forensic framework is also a generic cloud service stack that comprises the platforms as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS).

The main contributions in this paper are listed as follows:

(1) We have provided a comprehensive analysis of available forensic process models to illustrate their strengths and weakness points. We have discussed the steps and provided the functions of these models. Because cloud forensics is a branch of digital forensics, and most of the cloud forensic models are elaborated and developed digital forensic models and approaches, we have studied both the general digital forensic and cloud forensic models.

(2) We have presented a Forensic-enabled Security as a Service readiness framework (FESaaS) that shows how sufficient it is when we aggregate the security as a service layer and forensics layer. This framework will be helpful for cloud forensics experts to collect evidence instantly.

The rest of this paper is structured as follows: Section 2 presents a literature review. Section 3 provides a broad comparative study of various digital forensic frameworks. Section 4 gives short summaries about security as a service and forensics as a service. Section 5 defines our proposed framework and discusses its advantages. Finally, Section 6 concludes this study.

2 Literature Review

In the literature, several digital forensic process models have been presented for the cloud environment. In [6], a Digital Forensic Readiness (DFR) approach is used in the Cloud Forensic Readiness (CFR) model. The model shows a proactive forensic approach based on the active monitoring, collection, and retention of digital data within the cloud environment. The major purpose of CFR is to collect relevant digital data that exists as Potential Digital Evidence (PDE) that can be of use in supporting or refuting a hypothesis with a base on the occurrence of a digital event. The essential information gathered may include access logs, networks, hypervisor logs, and activity logs.

The CFR model can also consist of Non-Malicious Botnet (NMB) and the Cloud Service Provider (CSP)" infection." It is worth noting that "infection" in this context involves the modification of the initially-considered malicious botnet to gather digital information that has a positive connotation. The CSPs will give virtual services to the cloud users where a proactive NMB harvests digital information that can be used as potential evidence. This is indicated by the arrow pointing downwards and marked as a proactive process. The evidence that CFR remains is preserved and retained digitally for DFR purposes [7].

In the previous work provided by [8], the NMB is obfuscated for avoiding deterrence based on the botnet infiltration and detection strategies. There has been a proposal for event reconstruction processes at the scenes of digital crime. However, it has not been very effective as more attention has been directed to the physical crime scene and not from the perspective of digital forensic readiness in the cloud [9].

Furthermore, a research documentation by Carrier and Spafford [10] highlights the need for recognizing and collecting evidence at the crime scene at the beginning of the event reconstruction process. The authors further present the reconstruction process in five phases: Evidence examination, event construction

and testing, role classification, event sequencing, and hypothesis testing. Through these phases, the authors identify an object as the initiator causing a particular event to occur with the use of a role-based event reconstruction model.

Liao and Langweg [11] propose in their research a resource-based activity or the event re-construction of digital crimes prototype, including a readiness phase that helps to ensure that the evidence is admissible. The prototype has a correspondence with the DF framework and includes the following phases: readiness to collect system call traces, deployment phase to receive detection alerts, and investigation phase to preserve and recognize evidence and reconstruct events.

3 Comparison of Cloud Forensic Models

Forensic practitioners and researchers have proposed many Cloud forensic frameworks. Martin and Choo [12] presented an integrated cloud computing conceptual digital forensic framework that consisted of presentation and examination, preservation and evidence source identification, collection, and presentation, and reporting phases.

In their proposed framework, the third phase iterates back to the first phase in case more evidence or data is required. Pichan *et al.* [13] presented a cloud computing digital forensic model consisting of identification, preservation, examination and analysis, Collection or acquisition, as well as presentation. In their sub-process activities description, Pichan *et al.* also addressed the challenges and solutions recommended in each phase of the process. Furthermore, Zawoad *et al.* [14] proposed the process of computer forensics model for the cloud that consists of identification, organization, collection, and presentation. Their paper examined cloud forensic issues and challenges in every phase of the process proposed. However, Kent *et al.* [2] presented the National Institute of Standards and Technology (NIST) forensic model, which consists of collection, examination, and reporting and analysis phases.

In his work, McKemmish [15] presented the model of forensic computing that consisted of identification, presentation, and analysis phases. Shan and Malik [16] also proposed a framework of digital forensics for cloud computing that consisted of identification, collection, and preservation of data, as well as presentation and analysis phases. They illustrated the challenges as they suggested solutions in each of the phases of the framework. To further the idea, Quick and Choo [17] proposed an analysis cycle and iterative model of digital forensics consisting of commencing preparation and response, identification and collection, preservation, analysis, presentation, feedback, and completion. The paper [18] also put forward forensic processes consisting of identification, acquisition/collection and preservation, processing/examination and analysis, and results in dissemination phases.

The proposed process of forensics in this study combined the three forensic frameworks of Martin and Choo, Pichan *et al.*, and Shah and Malik in improving a successful cloud environment for forensic investigation. Although the purposes and the names of the phases proposed in this paper are similar to Martin and Choo, Pichan *et al.*, and Shah and Malik, the flow process adopted by every phase is different.

For instance, in the second phase, the two steps of collection and preservation are combined into a single phase and thus flow similarly to that of Shah and Malik. Moreover, the process flow carries out the collection step first followed by the preservation step.

On the other hand, Martin and Choo and Pichan *et al.* conducted the collection and preservation steps in different phases, beginning with the preservation phase and followed by the collection phase. Also, it is similar to Martin and Choo in the iteration from phase to phase that is examination and analysis to phase identification respectively. This paper also develops a forensic process as a service (FPaaS) by the use of cloud-based BPEL combining the four services/phases (collection and preservation, identification, analysis, and examination, as well as dissemination of results) into a brand composite service known as FPaaS [19].

Table 1 and Table 2 show the results of a comprehensive comparative analysis of different digital forensic frameworks. Table 1 analyzes the steps that each model follows, and Table 2 studied various functions that each model provides. The frameworks that have been investigated and discussed were proposed in the previous discussed literature in this section, as well as some additional studies, [20], [21], [22], [23], [24].

3.1 Discussion

Even though several digital forensic frameworks have been proposed for the cloud environment, still there are many challenges that these frameworks did not address. We have discussed some of them in this section.

As there is a connectivity of large resources to the cloud, the crime impact and investigation workload can be massive. For the timeline construction of the event, accurate synchronization of time is needed. The synchronization of time can be complicated because

Table 1. Steps that each forensic framework follows

Authors	Prepare & Respond	Identification	Collection	Examination	Preservation	Analysis	Presentation	Feedback
Martin & Choo		X	X	X	X		X	
Pechan *et al.*		X	X	X	X	X	X	
Zawoud *et al.*		X	X			X	X	
Kent *et al.*			X	X		X	X	
McKemmish		X			X	X	X	
Shan & Malik		X	X		X	X	X	
Quick & Choo	X	X	X		X	X	X	X
Popovsky *et al.*		X	X	X		X	X	
Grobler & Louwrens			X	X	X	X	X	
Siblya *et al.*		X	X		X	X	X	
Lei & Cui		X	X	X		X		
Hargreaves & Patterson		X	X	X		X	X	
Rowlingson	X	X	X	X	X	X	X	

Table 2. Functions that each forensic framework provides

Authors	Investigating	Troubleshooting	Log Monitoring	Data Recovery	Regulatory Compliance	Corporate Applicability	Law Enforcement Application
Martin & Choo	X	X	X	X	X	X	X
Pechan *et al.*	X	X		X	X	X	X
Zawoud *et al.*	X	X		X	X		X
Kent *et al.*	X		X	X	X	X	X
McKemmish	X	X		X	X	X	X
Shan & Malik	X		X	X	X		X
Quick & Choo	X	X	X	X	X	X	X
Popovsky *et al.*	X	X		X	X		X
Grobler & Louwrens	X	X	X	X	X	X	X
Siblya *et al.*	X		X	X	X	X	X
Lei & Cui	X		X	X	X	X	X
Hargreaves & Patterson	X		X		X		X
Rowlingson	X	X		X	X	X	X

the required data resides on various physical machines that are located in different geographical regions, with different remote web clients, on various equipment, and within several endpoints.

Log formats consolidation is another big issue of cloud forensics just like time synchronization, which becomes more difficult due to scaling issues in the cloud. It is also difficult to consolidate the logs or make them cross-compatible with each other due to huge resources on the cloud. Another big problem is that most of the providers create their proprietary formats of logs intentionally which causes roadblocks during investigation [14]. This is a problem because the proprietary formats of logs may not be interpreted with open-source tools. Furthermore, using disparate formats of logs is a challenge faced by the traditional forensics of networks. This is due to the large volume of logs of data as well as the proprietary formats of the log.

As mentioned before, in the cloud forensics organizational dimension, many cloud applications and CSPs depend on other CSPs. For example, a CSP

providing an application for email might be dependent on the provider of a third party for hosting log files. That third party might rely on other partners that provide infrastructure for storing the log files. Thus, a cloud forensics investigation might require the investigation of all the individual links which are present in the chain of dependency. Another challenge is the correlation of activities across various CSPs. Problems can arise due to a lack of coordination or an interruption as a cloud service may use different services of various cloud services provided.

Additionally, the data deleted is one of the most important evidence sources in digital forensics. In the case of cloud usage, each customer has the right to delete or alter the data if s/he has created it. When a datum is deleted by the customer, mapping in the domain happens immediately and is generally completed within a few seconds. Accessing the deleted data remotely is impossible without mapping. The space created by deleting the data is available for the new write operation and it is overwritten by the new data. However, there is a chance that the deleted data is present in the snapshot of memory. The challenges, in this case, deal with the recovery of the deleted data for identifying the ownership and use of the deleted data for reconstructing the event in the cloud [25]. Furthermore, due to the limited transparency of CSP, a lack of international regulation, and a lack of customer awareness, Service Level Agreements (SLAs) remove the important terms with respect to forensic investigation. Most of the customers of clouds are not aware of the issues or significance of the investigation of cloud forensics. Also, CSPs are not willing to increase transparency due to the lack of expertise related to legal or technical issues and a lack of regulations defined for increasing transparency [13].

4 Forensic and Security as a Service

4.1 Forensic as a Service

Digital forensic services can be accessed at any time needed, and a cloud provider may choose to invoke its service from the time of deployment of their cloud throughout the lifetime of the service. Providers can also release or instantiate it at any moment during the service lifetime. During lifetime service delivery, a need for investigation for the digital forensic services may arise at any moment, and since it is unpredictable, relevant information needs to be available for the investigation process. Thus, digital forensic service requires instantiation from the deployment of the PaaS to reduce the time and cost involved during the investigation process. Traditional digital forensic processes begin after the incident occurs when forensic experts start working to gather information. One of the main disadvantages of this process is it may involve a lot of time and money. For cloud environments, the post-incident investigation cost can be very high. Despite having a complex architecture, cloud forensic investigators can have remote access if the cloud provider allows [26].

4.2 Security as a Service

The cloud model provides three service models which include platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS). Depending on the cloud service level, the security service requirements will differ. As a service provider, the security service requirement of infrastructure may end up at the network level. Requirements for a service provider platform may as well end up at the information service level of security. On the side of the digital forensics service, the compatibility requirements for Software as a Service provider can be limited to the application activities and the platform deploying their services. Even if the IaaS providers can access the SaaS and the PaaS hosted on their environment, they can still forego limiting their digital forensic needs and responsibilities [26, 27].

5 The FESAAS Framework

5.1 FESaaS Framework

In our proposed Forensic-enabled Security as a Service (FESaaS) framework, the Security as a Service layer and Forensic as a Service Layers are aggregated to enhance the process of forensic analysis. Figure 1 illustrates the FESaaS framework.

The security as a service layer is divided into four logical layers, the application layer security, network layer security, physical layer security, and other security layers.

The application layer offers security devices such as web applications, binary analysis, firewalls, binary scanners, and security scanners [9]. Among them, the security devices may as well include virus definition updates, security and administrative tasks, and content security expertise.

Network layer security is very important in cloud forensic components as this layer of security is vital for the provision of IaaS, SaaS, and PaaS. This layer allows the virtual machine or instances connected to the cloud network. On the other hand, IaaS has cloud-hosted servers and devices connected via physical networks. The virtual networks that connect virtual machines are bridged over the IaaS physical network as well. In either of the cases, the data captured is always the same. The difference only comes in that the virtual network connections occur through vir-

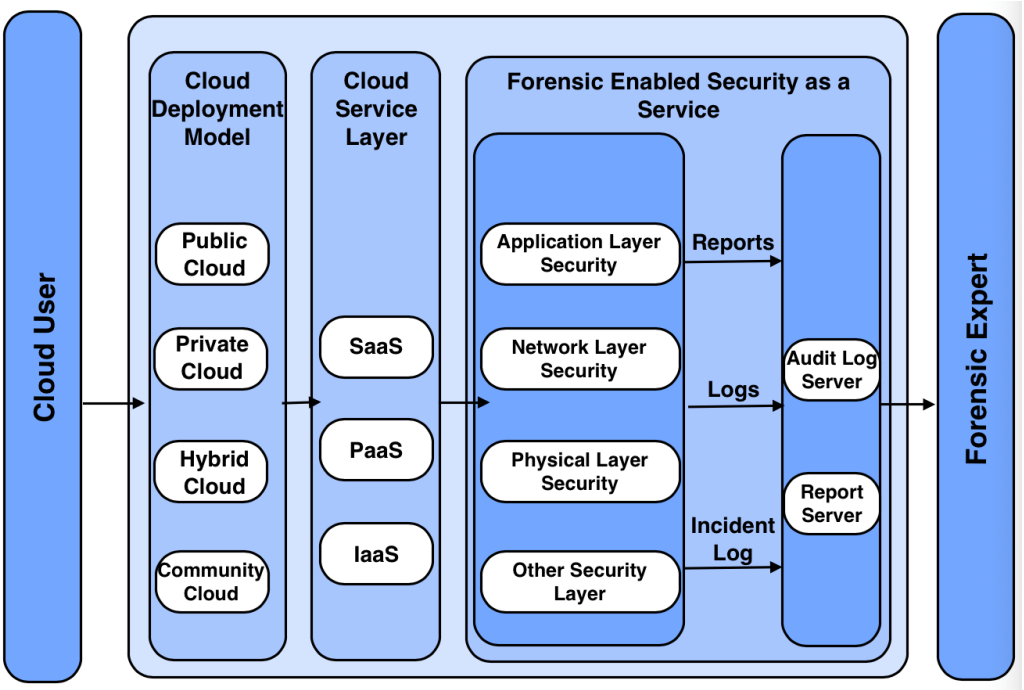

Figure 1. Forensic-Enabled Security as a service framework (FESaaS)

tual devices like virtual switches. The data captured by the network service components include IDS and IPS logs, as well as network logs. Such logs are essential when determining machines and devices that are disconnected or connected at any moment during the lifetime performance of the network. Hence, it is advantageous to have such data managed externally since it can still be retrieved in case the network is compromised during failure or attack [9].

The physical layer represents the physical security of the cloud. It consists of hardware resources with all the tools of cloud computing, which include network devices, processing facilities, terminal devices, storage devices, etc. All the instances are part of physical layer security. The CSP uses pooled resources for servicing the large request of consumers and uses dynamic allocation with different virtual and physical resources that are dynamically assigned or reassigned according to the request of users.

Security services on storage and compute layers provide security solutions for the storage devices and the host. These cover solutions such as encryption and firewalls. On trusted computing, security devices are mainly concerned with the APIs interacting directly with hypervisors. The network-level services include data packet inspection, firewalls, intrusion prevention, and intrusion detection. Additionally, the management level offers vulnerability assessment, patch management, identity management, vulnerability management, and access management. Security services offered at the information level are database monitoring activity, content filtering, content monitoring, and data leak prevention [9, 10].

For cyber crimes, it is crucial to present the evidence to the legal authorities. Figure 2 shows the process of representing the evidence to legal authorities. The CSP or third party can adapt the FESaaS model in their cloud environment. If concerned cloud users ask for evidence, the forensic expert will gain access from the FESaaS providers and be responsible to provide the forensic report to the user. Similarly, legal authorities can be given access to the evidence. Furthermore, forensic investigators can represent the evidence that will be filed with the court by acquiring forensic data from the FESaaS model. Everything depends on the CSP. If the CSP allows then the access can be given to the legal authorities. Moreover, the technical team may require acquiring evidence and logs on technical faults. This model is capable of providing evidence to the technical team as well.

The major players in the cloud environment are the applications that interact with layer 7 of the ISO/OSI model, such as dynamic and static web applications, web services, web clients, web services, and application services. The layers are also the means of the exchange of data throughout the world between servers and clients. The applications are connected by a new set of applications between the cloud which offer collaborative conditions such as Integrated Development Environments (IDEs) and online work processors. Therefore, the latter application can hence be used as a rich data source for investigation pur-

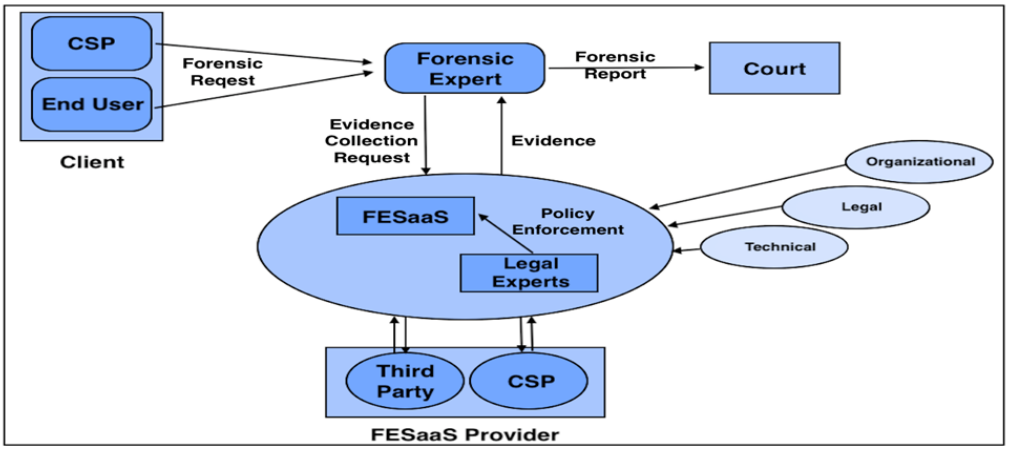

Figure 2. The process of representing the evidences to authorities

poses. SaaS has evolved from the application service provider model of software hosting and is thus considered the most mature category of cloud services.

In a cloud environment, software offered as a service is a single instance of the application which is also hosted by the provider. Customers or users access it from just a single server as their unique configurations and data are virtually partitioned from other users. In the instance of creating a deployed application, the cloud platform dynamically determines the server to enable the running of the instance. In that case, digital forensic service is used in keeping track of information to enable its use for investigation purposes. Log files associated with the running application from the servers are retrieved at varying intervals as per the digital forensic consumer determination [9].

The RAM Forensics is mainly used by the PaaS providers as it is responsible for application data access that belongs to the application hosted as a service and the information regarding their platform. The PaaS providers install their custom applications and platforms on virtual machines that are deployed on IaaS. PaaS providers then manage the virtual machine on which their platforms are running. Upon being invoked, the digital forensic service takes snapshots of the running virtual machines hosting the platform. At the exact time the data was captured, the snapshot preserves state data for virtual machines. The state information will hence indicate whether the virtual machine was suspended, running, or shut down. The data collected includes disks as well as all other devices connected to the virtual machine. The layer of middleware component serves basic functionality of platform of cloud computing in order to ensure that the services of cloud are optimally installed, maintained and delivered. It also includes resource management, user management, safety management, and task management [18, 28].

The major part in this model is the Forensic layer. As mentioned above, all the security layers produce logs, incident logs, and reports. In this proposed model, all the logs will be stored in an audit log server and the cloud forensic investigator can be given access to the log servers remotely. The cloud forensic investigator can easily analyze the log data for forensic purposes. The log data investigation phases include the data analysis, data acquisition, data bookmarking, data filtering, report generation and Hex data viewing.

5.2 Advantages of our Framework

This model improves the cloud investigation process. It improves the security of Cloud systems and also ensures a prompt forensic analysis. Moreover, any forensic analysis tool can be used by the investigator from the obtained logs and report data. This will improve the timeline of the forensic tools. Even if some data is lost or fails, the authenticity and integrity of forensic data will remain protected. As the analysis will be mostly on live data there will be no instant requirement of offline data. Furthermore, that will reduce processing time of both client and server side as the normal cloud service process will work as usually. Another advantage is the easier information integration and resource sharing. It will use the security as a service layer for logs and incident data. Every security application creates logs. Log and report servers will store the log data. This model uses virtualization technology and all resources provided in the software of up-per application in transparent way. The cloud computing process stores user data in cloud storage which removes the need for physical access. One of the major advantages of this model will be ensuring the CIA (Confidentiality, Integrity and Availability) Triad. The elements of the triad should be guaranteed in any type of secure system. Serious issues might

be raised when any of these three security goals is not be considered. The following points describe how CIA is maintained in our model.

- Confidentiality: It is the secrecy of important data of any organization, only some authorized people can access that data. That type of security is known as confidentiality of the security system. An authorized person is a specific and trusted person in an organization who can access critical data. In this framework, forensic investigators will have access to reports and log servers only. They will not have any access to the client data or core data. Thus, CSP will ensure safe access to the client data.
- Integrity: This means the excellence of information and the goal is to maintain important information from being altered. The process of checking errors and corruption in the information and correcting them is known as the integration of the information. As we have mentioned, this framework works on log data only; it works with live data without changing anything. Although forensic process may require investigating the offline data, this proposed framework will mainly deal with the live data and work as a ready model.
- Availability: The meaning of availability in terms of Information Security is to make the use of information of any organization at an advantageous time for one or some specified persons. Authorized people of an organization can access the important information whenever they want, and our framework ensures the availability of data. The forensic layer will be accessed by the forensic investigators or forensic administrators.

6 Conclusion

Nowadays, most sectors depend on technology and many companies have shifted to cloud-based services due to COVID-19. Therefore, the need for sufficient cloud forensic approaches has become a significant requirement. We need a forensic model that can help to find evidence for cybercrime, to create audit reports on incidents, and to submit court evidence. This paper proposed a framework that uses existing security services to provide a feasible, prompt, and effective cloud forensic mechanism. This framework primarily deals with live data, reports, and logs and will help forensic investigators to identify the root causes of cybercrime incidents. Our framework is suitable for prompt identification of the root causes as well. The proposed framework is helpful for both private and public clouds. Future work will be on broader spectrum; there are many cloud forensic aspects that need improvement.

References

[1] T Charles and M Pollock. Digital forensic investigations at universities in south africa. In *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, pages 53–58. IEEE, 2015.

[2] Tasleem Sulthana and Digambar Pawar. Digital forensic investigator for cloud computing environment. In *Computer Communication, Networking and IoT*, pages 53–61. Springer, 2021.

[3] Omi Aktera, Arnisha Aktherb, Md Ashraf Uddinc, and Md Manowarul Islamd. Cloud forensics: Challenges and blockchain based solutions. *Journal of Modern Education and Computer Science*, 10(8):1–12, 2020.

[4] James Baldwin, Omar MK Alhawi, Simone Shaughnessy, Alex Akinbi, and Ali Dehghantanha. Emerging from the cloud: A bibliometric analysis of cloud forensics studies. In *Cyber threat intelligence*, pages 311–331. Springer, 2018.

[5] George Sibiya, Thomas Fogwill, Hein S Venter, and Sipho Ngobeni. Digital forensic readiness in a cloud environment. In *2013 Africon*, pages 1–5. IEEE, 2013.

[6] Victor Kebande and HS Venter. A functional architecture for cloud forensic readiness large-scale potential digital evidence analysis. In *European Conference on Cyber Warfare and Security*, page 373. Academic Conferences International Limited, 2015.

[7] Victor R Kebande and HS Venter. Cfraas: Architectural design of a cloud forensic readiness as-a-service model using nmb solution as a forensic agent. *African Journal of Science, Technology, Innovation and Development*, 11(6):749–769, 2019.

[8] Victor R Kebande and Hein S Venter. A cloud forensic readiness model using a botnet as a service. In *The international conference on digital security and forensics (DigitalSec2014)*, pages 23–32. The Society of Digital Information and Wireless Communication, 2014.

[9] Victor R Kebande and Hein S Venter. Adding event reconstruction to a cloud forensic readiness model. In *2015 Information Security for South Africa (ISSA)*, pages 1–9. IEEE, 2015.

[10] Brian Carrier and Eugene Spafford. An event-based digital forensic investigation framework. *Digital Investigation*, 2004.

[11] Yi-Ching Liao and Hanno Langweg. Resource-based event reconstruction of digital crime scenes. In *2014 IEEE Joint Intelligence and Security Informatics Conference*, pages 129–136. IEEE, 2014.

[12] Ben Martini and Raymond Choo Kim-Kwang. An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, 9(2):71–80, 2012.

[13] Ameer Pichan, Mihai Lazarescu, and Sie Teng Soh. Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital investigation*, 13:38–57, 2015.

[14] Shams Zawoad and Ragib Hasan. Cloud forensics: a meta-study of challenges, approaches, and open problems. *arXiv preprint arXiv:1302.6312*, 1, 2013.

[15] Rodney McKemmish. *What is forensic computing?* Australian Institute of Criminology Canberra, 1999.

[16] JJ Shah and Latesh G Malik. An approach towards digital forensic framework for cloud. In *2014 IEEE International Advance Computing Conference (IACC)*, pages 798–801. IEEE, 2014.

[17] Darren Quick and Kim-Kwang Raymond Choo. Digital droplets: Microsoft skydrive forensic data remnants. *Future Generation Computer Systems*, 29(6):1378–1394, 2013.

[18] Amna Eleyan and Derar Eleyan. Forensic process as a service (fpaas) for cloud computing. In *2015 European Intelligence and Security Informatics Conference*, pages 157–160. IEEE, 2015.

[19] Cornelia P Grobler and CP Louwrens. Digital forensic readiness as a component of information security best practice. In *IFIP International Information Security Conference*, pages 13–24. Springer, 2007.

[20] Barbara Endicott-Popovsky, Deborah A Frincke, and Carol A Taylor. A theoretical framework for organizational network forensic readiness. *J. Comput.*, 2(3):1–11, 2007.

[21] George Sibiya, Hein S Venter, and Thomas Fogwill. Digital forensic framework for a cloud environment. pages 1–8, 2012.

[22] Yunting Lei and Yuyin Cui. Research on live forensics in cloud environment. In *2nd International Symposium on Computer, Communication, Control and Automation (3CA)*. Citeseer, 2013.

[23] Christopher Hargreaves and Jonathan Patterson. An automated timeline reconstruction approach for digital forensic investigations. *Digital Investigation*, 9:S69–S79, 2012.

[24] Robert Rowlingson et al. A ten step process for forensic readiness. *International Journal of Digital Evidence*, 2(3):1–28, 2004.

[25] Nasir Raza. Challenges to network forensics in cloud computing. In *2015 Conference on Information Assurance and Cyber Security (CIACS)*, pages 22–29. IEEE, 2015.

[26] Jooyoung Lee and Sungyong Un. Digital forensics as a service: A case study of forensic indexed search. In *2012 International Conference on ICT Convergence (ICTC)*, pages 499–503. IEEE, 2012.

[27] Vijay Varadharajan and Udaya Tupakula. Security as a service model for cloud environment. *IEEE Transactions on network and Service management*, 11(1):60–75, 2014.

[28] Karen Kent, Suzanne Chevalier, and Tim Grance. Guide to integrating forensic techniques into incident. *Tech. Rep. 800-86*, 10(14), 2006.

Wedad Alawad Received the B.Sc. degree in Computer Science from Qassim University, Saudi Arabia in 2008, and the M.Sc. degree in Computer Science from Bowling Green State University, United States in 2014, and Ph.D. degree in Computer Science from Oakland University, United states in 2018. She is currently an assistant Professor of Computer Science at Qassim University, Saudi Arabia. Her research activity is related to artificial intelligence, cyber security, and cloud computing

Awatef Balobaid Received the B.Sc. degree in Computer Science from Taibah University, and the M.Sc. degree in Computer Science from Bowling Green State University, United States, and Ph.D. degree in Computer Science from Oakland University, United states . She is currently an assistant Professor in the Department of Computer Science, Jazan University, Saudi Arabia. Her research activity is related to Internet of Things, cyber security, and cloud computing.