Digital Forensics Framework in Cloud Computing Service SaaS

Arwa Almohammdi[1†] **Nermin Hamza**[2†] **Shireen Saifuddin**[3†],
asaadalmohammdi@stu.kau.edu.sa nermin.hamza@cu.edu.eg ssaifuddin@kau.edu.sa
Faculty of computing and Information Technology, Jeddah – Saudi Arabia [1†3],
Faculty of graduate studies for statistical research, Cairo university[2†].

Summary
Nowadays, cloud computing has become a prominent, widespread and popular technology as a convenient and cost-effective computing paradigm. Nevertheless, the architecture of cloud computing lacks support for investigations of forensic and security. Due to the virtual and distributed cloud nature, malicious activities can be carried out very easily and at the same time, it is so hard to investigate. Recently, cloud forensic investigators have encountered several problems, such as the lack of forensic techniques and tools in the cloud environment. This highlights the need to develop a new cloud forensics framework aimed at mitigating the challenges. This paper presents a framework for digital forensics in software-as-a-service (SaaS) cloud environments. It simulated the framework on Nextcloud that uses client-server software for file hosting services as a case study. The proposed framework has been assessed by validating it against the published report of the National Institute of Standards and Technology on the Forensic Challenges of Cloud Computing (NISTIR 8006). Further, it has been validated by two criminal cases. The investigational results proved that the proposed system could assist digital investigators in their mission of investigating cybercrimes in the cloud in a proficient manner and mitigate many challenges, such as the dependency on cloud service providers and collecting deleted data from the cloud section.

Keywords:
Digital Forensics, Cloud Computing, Cloud Forensics, SaaS, Investigation.

1. Introduction

During the last few years, cloud computing has revolutionized the way in which digital information is stored, communicated, and processed. Cloud computing is not just a hyped technology; it has been embraced by Information Technology (IT) giants like Amazon, Google, Apple, HP, IBM, and Oracle. Recently, many people have come to regard the concept of cloud computing as a revolutionary new IT paradigm, considering it to be industry-changing and one of the fastest-growing technologies since the invention of computing itself [1]. According to Grand View Research [2], the global cloud computing market was worth USD 274.79 billion in 2020 and will expand at 19.1 % Compound Annual Growth Rate (CAGR) from 2021 to 2028. This demonstrates the rapid expansion of the cloud computing industry and the rise in the number of cloud users throughout the world. This expansion has led to an increase in the frequency of cybercrimes, offending behaviors that involve the use of the internet or a computer as a means of committing offenses [3]. Cyberattacks are increasingly targeting cloud services and data centers, raising security concerns [4]. In addition, as a result of the COVID-19 pandemic, many businesses, managers, and employees have moved to remote working, and it is predicted that many will choose to continue the practice in the long run, making this the new trend a critical workplace shift [3]. However, the greater population and alternative working environment have significantly increased the need for cyber security and forensics investigations. According to a report by the Cyber Threat Global Risk Index, cyberattacks are steadily elevating to the status of a global risk factor [11].

Furthermore, now that Cloud Services Providers (CSP), such as Dropbox, Google Drive, Amazon Cloud Drive, SpiderOak, Ubuntu One, and Apple iCloud, offer remote storage capabilities, cybercriminals can store confidential data and files, such as forged documents and pornographic images, in cloud storage and erase all digital evidence from their local storage; this enables them to escape detection if they are investigated [3]. When looking into cybercrimes involving cloud computing platforms, investigators need to conduct digital forensic investigations on both the suspected client device and in the cloud computing environment.

According to Ruan et al. [5], “A crime that involves cloud
computing in the sense that the cloud can be the object, subject, or tool of crimes (object - Cloud Service Provider (CSP) is the target of the crime; subject - the cloud is the environment where the crime is committed; tool - the cloud can also be the tool used to conduct or plan a crime”. Cybercriminals may use many types of attacks, such as Distributed Denial-of-Service (DDoS) attacks, to target the CSP, or they may use the cloud environment to commit crimes, such as illegally accessing data stored in the cloud, stealing the identity of a cloud user, or using the cloud as a location to store and share illicit information with others.
Researchers have also pointed out that the cloud infrastructure is not mature enough to support digital forensic needs because distributed cloud environment [6]. Even though cloud forensic investigations have moved forward in recent years, there are still open issues to explore, and many challenges need to be resolved to facilitate an

Manuscript received November 5, 2022
Manuscript revised November 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.11.76

appropriate investigation related to cloud forensics. Significantly, Software as a Service (SaaS) cloud services still needs to experiment with many applications and identify a framework that addresses some of its challenges. The SaaS model especially involves the central hosting of the program and the data it needs in a cloud computing environment. moreover, its multi-tenancy design framework. When several users are served by a single instance of software operating on a server, this situation is referred to as multi-tenancy (tenants) [12]. Thus, the user does not have control over the underlying operating infrastructure, such as the network, servers, operating systems, or even the utilized application. This implies that the client is not given a more detailed picture of the system and its underlying architecture [7]. There are just a few user-specific program configuration parameters that may be controlled such as user interface. This forces the investigator to rely on high-level logs, which the CSP ultimately gives in many situations. Therefore, investigators have no way of generating any relevant evidence on their own. It is impossible to install or configure any toolkit or logging program [8]. Thus, these factors preclude a meaningful forensic investigation, meaning that SaaS investigators have no way of analyzing possible incidents. Also, investigators in a cloud environment must depend on the CSP to carry out their forensic activities. Consequently, the CSP is the most important role actor since it is in control of all data and information. In order to obtain network and server records, investigators must also rely on the CSP, and there is a chance the CSP could tamper with the logs [9]. Moreover, in SaaS digital forensics, many challenges are faced, such as multi-tenancy, unknown physical locations, inaccessibility, multi-jurisdictions, deleted data, and decentralized data [10]. Due to the SaaS access-control level, forensic investigators experience enormous challenges in dealing with illegal actions, which are not as complicated in other cloud services [13]. That is because it fully relies on CSP.

This paper proposed the framework, "Digital forensics framework in cloud computing services," that would help make it easier to investigate illegal activities in cloud computing and provide a method to assist investigators in collecting and analyzing evidence outside the cloud place. The forensic steps proposed in this study can be scaled to cloud data to handle cloud-related criminal investigations. The proposed framework would help digital forensic investigators to minimize the overall challenges in cloud crime. The remainder of the paper is organized as follows: Section II is about related work, section III described the proposed framework design, section IV explained in detail the implementation and experiment environment. Section V presented results analysis and discussions, and then in section VI conclude the paper.

2. Related Work

The importance of digital forensics has increasingly attracted the focus of researchers. Several valuable works have attempted to investigate digital forensic cloud computing services. Many researchers have helped to identify forensic challenges, create some of the proposed forensic frameworks, and establish data-gathering methods for cloud computing systems but still, there are several challenges that required to be inspected.

There are three cloud service models related to the services provided by CSPs [9]: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and SaaS. This paper focused on SaaS challenges. In light of SaaS challenges introduced in [16] and [6], They analyzed the forensic investigator's needs and proposed a framework dependent on the cloud log framework. Khan et al [16]. proposed a forensic analysis of a cloud environment by combining logs from the CSP and client-side to help identify suspicious activities on cloud-based systems. While Pichan et al. [6] proposed log framework helps trace any malicious activity whenever users have finished using their cloud services.

Other forensic frameworks proposed within the SaaS area focus on applications, event logging, and networks [14] and [15]. Alex et al. proposed a new model for mitigating the challenges in cloud forensics outside of the cloud environment by creating a Forensics Monitoring Plane (FMP) that captured cloud logs and connections. On the applications side, Daryabar et al. [15] proposed a forensic framework. They identified a set of artifacts derived from clients' activities, such as downloading, uploading, log-in, deletion, and file sharing on iOS and Android devices to build evidence.

The above papers consider the cloud logs as an important resource to build evidence. After the analysis, we remark that most of the proposed works still depend on CSP for collecting cloud data and logs.

Over the last few years, many researchers have helped to identify forensic challenges, create forensic frameworks, and establish data-gathering methods for cloud computing systems. In general, while these works have identified the technical, organizational, and legal challenges of cloud forensic analysis, no concrete solutions to the challenges of applying forensics to the cloud environment have been proposed that are acceptable to forensic investigators or Law Enforcement Agencies (LEAs) in this digital space. As a result, there is a pressing need to conduct large-scale forensic research on the cloud. The primary challenges of cloud forensics stem from the features used to identify the cloud computing platform. Beyond these challenges, there is still a lack of research in the cloud forensics area and other issues warranting additional study. These issues include accessing data located within the cloud and analyzing them, as most previous works depended on the CSP for collecting log data. Also, the investigation process is faced with

challenges concerning the nature of cloud computing, which is a multi-tenant environment that makes collecting deleted data difficult after users have terminated their services.

3. Proposed Framework

The critical analysis of the related work discussed in the previous section notes that most previous frameworks are applied and implemented in the cloud and depend on CSP for investigation and collecting logs data. It recognizes the need for a framework that applies outside the cloud place and is less dependent on CSP. Due to a lack of work at the SaaS level and to overcome its challenges, such as CSP controls the cloud resources.

This paper proposed a new framework for digital forensics in SaaS cloud computing. The proposed framework aims to build evidence by collecting and analyzing cloud data without depending on CSP. Also, it offers direct access to cloud logs data and user activities anywhere/anytime stored in a forensic server without any chance of meddling with evidence. Furthermore, the proposed framework is designed to provide a comprehensive solution to exceed most of the cloud forensics challenges, such as dependence and trust on CSP, duplicate data copies spread over changing virtual servers and unknown physical locations and collecting deleted data from a cloud section after the user finished its usage.

Proposed cloud forensics framework design is shown in Figure 1. The system architecture consists of six elements, which play fundamental roles in this framework. These elements are Client, Monitoring System (MS), SaaS cloud service, Forensic Server (FS), and log acquisition and integration, and analysis and reporting.

1)Client: sends a request to cloud service to access services such as login, create files, and upload files.
2) MS: has all the tools and techniques to monitor and capture all connections between different clients devices at an organization and remote cloud service SaaS.
3) SaaS Service: the services apps provided by the CSP such as Google Drive and OneDrive.
4) FS: the place where all data logs are collected.
5) Log acquisition and Integration: This phase collects and integrates all log files from the user's side and the forensics server side.
6) Analysis and Reporting: The analysis and reporting phase deals with all log data analyzed to find the required evidence and build a chain of custody report.

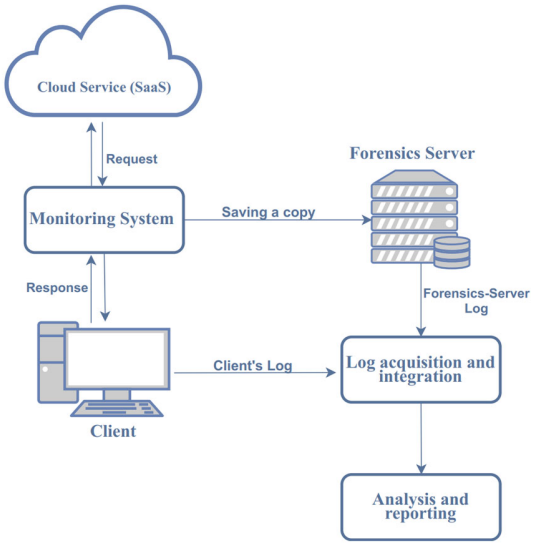

Fig.1. Proposed Cloud Forensics Framework Design.

The steps involved in the proposed framework are as follow:

• **Step 1**: The user starts a session and sends requests to the cloud service.
• Step 2: The request is intercepted by MS that forwards it to cloud service. At the same time, it is forensically imaged and saved to a forensic server.
• **Step 3**: Cloud service sends a response to the user, intercepted by MS, saves a copy in the forensics server, and sends it to the user at the same time.
• **Step 4**: An investigator is logging into the forensic server and collecting evidence for analysis.
• **Step 5**: An investigator collect sets of log files from the client's side. Then, processing with digital forensics tools.
• **Step 6**: The proposed framework analyzes Log data obtained from CSP and cloud sides by forensics tools to find and related evidence.
• **Step 7**: Investigator finds the required evidence and builds a chain of custody report appropriate to present in front of a court of law.

5. Implementation and Experimental Environment

To simulate the proposed framework for cloud forensics, the first step needs to build a virtual network environment. Figure 2 shows the virtualization network environment. It uses a Virtual Machine (VM) for creating a cloud computing network and software setup. The built simulation environment contains the Nextcloud app that

works as a cloud service, MS contains (Squid and Tcpdump) tools and different user devices. In the proposed framework is validated by two crime case studies that were used as proof of the concept's validation. After which the results were analyzed against NISTIR 8006.

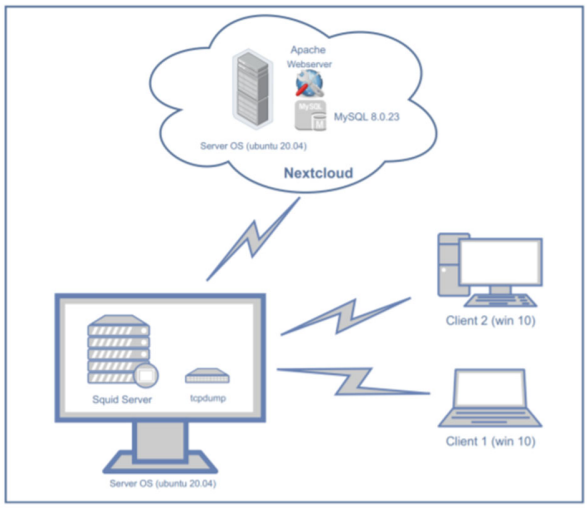

Fig.2. Simulation Environment

To represent the proposed framework on built cloud computing environment, we are following the steps simulation
below:
1) Created clients' accounts on Nextcloud, determined their permissions and connected them with the cloud server.
2) Finished MS settings and connect with all devices on the network: Cloud server, Clients devices, and FS.
3) Run the MS tools to capture all detailed information throw network, such as cloud logs, Network Traffic, request, response, then save on the FS.
4) performed crime cases study activity in different clients' accounts.
5) Collected data from FS and clients' devices for analysis by forensics tools to build the report.

5. Results Analysis and Discussions

5.1 Crime Case studies

This section describes the validation of the proposed forensic framework. For which two use cases involving different criminal cloud activities are presented as discussed by Pichan et al. [6].

5.1.1 First Crime Case Study

The first crime case study begins with the assumption that a malicious actor, referred to as a user-hacker, creates a user account, accesses cloud resources, and uploads malicious programs. The user-hacker then downloads malicious programs onto a target device to perform many ill-intentioned activities, such as harvesting credit card numbers and cracking passwords. By installing malicious programs on the target device, results are collected in a file and dispatched to the cloud. Finally, the user-hacker deletes his account and altogether terminates the cloud services. After an account on cloud infrastructure is deleted, the space is quickly reallocated to other users.

The results of First Crime Case Study
In the built simulation environment, proposed work started testing the first criminal case study scenario and applied every step by following simulation steps discussed in previous section. After the scenario ended, data was collected from the FS and client sides to analyze data and build evidence.

From The forensics server-side: Monitoring the first crime use case, FS was accessed to collect all related data by using the FTK Imager tool. After which the data were analyzed using a forensics tool to find evidence of criminal activity. The analysis of a screenshot shown in the figure 3 uncovered login to a user account from the IP address 192.168.8.10 and forwarding to a device with the IP address 192.168.8.1111 on Microsoft Edge. Also, as shown in the figure 4, a device with the IP address 192.168.8.10 displays the creation of a new folder named "Pwd Cracker". The same device conducted different activities from 1:14 a.m. to 2:32 a.m. on Tuesday, 01 January 2021. For example, the user uploaded an executable file called "Pwd Cracker.exe" downloaded an executable file. Also, it uploaded an XML file named "Pwd cracker.xml." Finally, the user logged out and deleted his account.

The client-side: For the second step, cloud log data from the client device was collected by the FTK Imager tool and then analyzed using the Autopsy forensics tool. It was observed in the user carried out different activities related to the criminal case scenario.
All remaining screenshots related to the first crime case study are provided in Appendix A (fig. 1–9). After analyzing data collected and imaged from the FS and client sides, the summary of results is presented in Table 1. The table has all the main information that the investigator needs to build the evidence report such as Which are the sender and receiver IP addresses, time and date of the cloud action, the action description, cloud service and the forensics tools used to collect and analyze these data.

5.1.2 Second Crime Case Study

The second crime case study is underlain by the supposition that a malicious actor called “user-evil” creates accounts for trading child pornography on the Internet. The malicious actor acquires and stores an extensive collection of pornography image files on his laptop. He uses a cloud computing environment as the best solution for distributing and storing photos and files without leaving traces of his actions. The malicious actor then creates an account on a cloud computing platform and acquires all the necessary space and storage to upload all the image files to the cloud. He uses special tools to erase all possible traces and locally wipes out the files from the machine. Once the job is completed, he rapidly terminates the account.

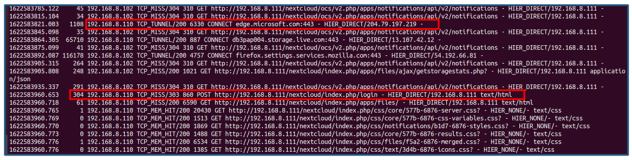

Fig.3. First crime case study (Login)

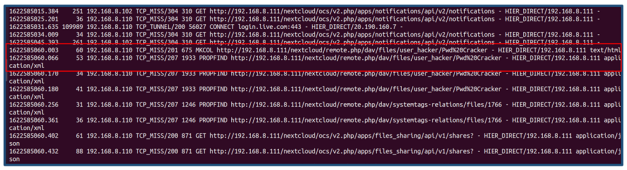

Fig4. First crime case study (Create Folder)

The results of Second Crime Case Study

The forensics server-side: First, the FS was accessed to collect all related data by using the FTK Imager tool. Then, the data were analyzed using a forensics tool to find evidence. In this criminal case, a device with the IP address 192.168.8.114 sent a request to a server with the IP address 192.168.8.111 on Thursday, 03 Jun 2021 to allow the user to log in the Figure 5. It was also found that a request from a device with the IP address 192.168.8.114 for the uploading of five image files: “Cat.jpg,” “Horse.jpg,” Movie.jpg,” “Penguins.jpg,” and “Magazin.jpg” on the User-Evil account. After that, the analysis results reflect that the same device shared all the photos to different accounts before deleting them. Finally, user completed his activity on the Nextcloud cloud service and logged out.

The client-side: For the client device analysis, an image of the client device using FTK Imager was created; then, the analysis process used the Autopsy forensics tool. The analysis process observed that the client’s device carried out actions relevant to the criminal case scenario.

All remaining screenshots of the second crime case study are shown in figures 10–21 in Appendix A. After analyzing data collected and imaged from FS and client sides, the summary of results is shown in Table 2. The table has all the main information that the investigator needs to build the evidence report such as Which are the sender and receiver IP addresses, time and date of the cloud action, the action description, cloud service and the forensics tools used to collect and analyze these data.

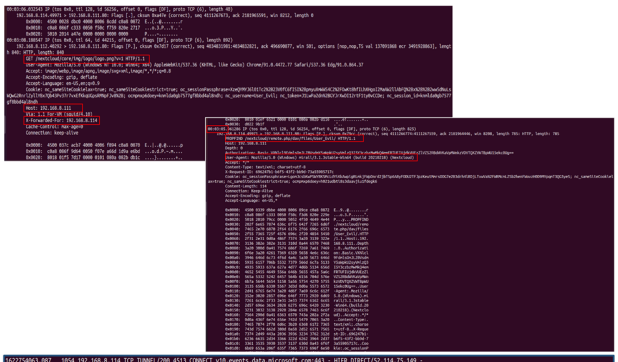

Fig.5. Second crime case study (Login)

5.2 Discussion

The purpose of the study was to find a framework that helps investigate the SaaS cloud service without relying on CSP and overcome cloud forensics challenges. The overall goal of creating a framework that decreases CSP roles was accomplished by building an FS located under an investigator’s control. Also, the study revealed a way to retrieve deleted data in a multi-tenant cloud environment by capturing all requests and responses between the cloud service and the client’s device by different tools on MS. The proposed framework assists in building trust and good evidence by collecting cloud data from FS and client sides. This work also allows for the collection of cloud data and related information whatsoever location or time zone. Thus, this leads to documenting a chain of custody paper without discrepancies or gaps.

The analysis of digital evidence related to the previous two criminal cases’ scenarios that were collected from both the FS and a client device found that there is evidence proving that a device with IP address 192.168.8.114 and another having IP address 192.168.8.10 are responsible for the crimes in the Nextcloud cloud service. This led to the conclusion that the proposed framework can help investigators and LEAs find data on criminal actions in cloud computing environments in a timely, efficient,

effective, and forensically sound manner. Also, the results indicate that the proposed framework provides a method to assist investigators in collecting and analyzing evidence and help digital forensics investigators to minimize the overall challenges of investigating cloud crime.

No	Sender IP Address	Receiver IP Address	Time	Date	Event Action
1	192.168.8.10	192.168.8.1111	01:16 AM	Tuesday ,01 January 2021	Login
2	192.168.8.10	192.168.8.1111	01:25 AM	Tuesday ,01 January 2021	Create a new folder "Pwd Cracker"
3	192.168.8.10	192.168.8.1111	01:30 AM	Tuesday ,01 January 2021	Upload an executable file "Pwd Cracker.exe"
4	192.168.8.10	192.168.8.1111	01:34 AM	Tuesday ,01 January 2021	Deals with executable file
5	192.168.8.10	192.168.8.1111	02:10 AM	Tuesday ,01 January 2021	Upload XML file " Pwd cracker.xml"
6	192.168.8.10	192.168.8.1111	02:32 AM	Tuesday ,01 January 2021	Logout

The proposed framework is practical enough because it can easily solve multiple challenges faced by digital forensics in cloud computing services. A large body of literature has investigated cloud forensics by depending on CSP, which affects the quality of evidence and the trustworthiness of investigation. For example, the authors in [16] and [6] proposed a cloud forensics framework suitable for the SaaS level but relying on CSP. The proposed framework overcomes this issue by building an FS located outside the cloud location. For building evidence from different data log resources, [14] and [6] proposed a framework for collecting cloud logs from only one side. The proposed framework instead suggests a way of collecting logs from both the FS and client sides. Moreover, researchers in [16] and [6] did not address the issue of collecting deleted data in a cloud environment. The proposed framework mitigates this challenge by establishing a monitoring system that captures all cloud data and stores it automatically on an FS. Also, none of the existing frameworks tries to use Nextcloud as a cloud service to test the framework.

Table 1: First crime case study results

Table 2: Second crime case study results

No	Sender IP Address	Receiver IP Address	Time	Date	Event Action
1	192.168.8.114	192.168.8.1111	00:03 AM	Thursday ,03 January 2021	Login
2	192.168.8.114	192.168.8.1111	00:16 AM	Thursday ,03 January 2021	upload five image files
3	192.168.8.114	192.168.8.1111	00:29 AM	Thursday ,03 January 2021	Shared all photos to different accounts
4	192.168.8.114	192.168.8.1111	00:41 AM	Thursday ,03 January 2021	Deleted all the photos
5	192.168.8.114	192.168.8.1111	00:50 AM	Thursday ,03 January 2021	Logout

To support cloud forensics the proposed framework provided other advantages include:

- Flexible location and time by collecting data from one location.
- Save a significant cost by centralizing the location of collecting digital forensic evidence.
- Data originality by directly stores data by MS.
- Ability to identify the attackers and criminals in cloud computing.
- Facilitating the digital investigation process in a cloud environment.

5.3 Analysis of the study results against NISTIR 8006

National Institute of Standards and Technology Interagency or Internal Report 8006 (NISTIR 8006) identifies and summarizes the cloud computing forensic science challenges [17]. Some of the cloud computing forensic science challenges that related to logs and data are:

1) **Deletion in the cloud**

Recovering deleted data from the cloud and attributing it to a specific user is challenging because it is a multitenant environment. The logging services are provided by CSPs but cannot trust them to share all related data. Also, it remains hard to attribute specific data to an individual user. In the proposed framework, all requests and responses from/to cloud server and network activity are stored on private and forensics servers automatically, mandatory, and persisted without any third party, thereby providing all data even if a user deleted his account.

2) **Recovering overwritten data**

In a shared virtual environment, once a user deleted his account, it will use the space to another user and will be overwritten on previous data. This considering a challenge to recovery of deleted data in this case even by CSP. In the proposed framework using the separate FS that captures all logs data constantly. This feature helps to track logs data even if a user deletes their account.

3) **Reconstructing virtual storage**

In some cloud computing environments, media imaging (virtual storage reconstruction from physical disk images) has an added level of complexity that leads to damage to the original media. An investigator in the proposed framework reconstructs virtual storage only on the forensics server to image all relevant physical disk images that easier to produce reliable and associated forensic evidence.

4) **Timestamp synchronization**

Synchronization of timestamps in network forensics is challenging in a cloud environment. Due to it being hard to synchronize over different physical machines that are spread over different geographical regions. In the proposed framework, collecting evidence from the forensics server helps and makes it easy to do data correlation and forensic analysis along a uniform timeline.

5) **Detection of the malicious act**

Attacks on computer systems are executed out of incremental steps, where each step exploits as a minor vulnerability in an attack. Also, cannot be noticed easily until the attacker penetrates and happens on the cloud and significant system. In the proposed framework, this could be done by capturing all requests and activity on the cloud network. It would be easier and faster than before to detect a malicious act.

6) **Errors in cloud management portal configurations**

In cloud management, portals configuration errors may result in an unauthorized user deleting or reconfiguring another user's cloud computing platform. In the proposed framework, track all network activities from/to cloud server helps to overcome this challenge. Also, it be more accessible for investigators to find the actual attribute of all changes. That changes originate from cloud management portal applications to a specific user. Resulting in the investigator knowing when an unauthorized user has gained control, reconfigured, or deleted another tenant's resources or applications.

7) **Multiple venues and geolocations**

Access to a cloud system and network resources include a wide area and maybe more than one venue and geolocation. Sequentially, it can impact finding evidence, chain of custody, and identifying required resources for access to the system. In the proposed framework, one forensics server can solve this challenge and easier to maintain the chain of custody.

8) **Data chain of custody**

Maybe impossible to verify a chain of custody because of the multi-layered nature of cloud computing. It is hard to determine precisely where the data was stored, who had access to it, and whether leakage or contamination of the data. In a proposed framework, all data is stored in an FS which is a secure place. Also, it is easy for the investigator to verify who had continuous ownership and access to forensic evidence in FS.

9) **Locating evidence**

Cloud computing is a changing and extensive system where E-discovery is essential for locating data when needed. In the proposed framework, all data is stored on the forensics server in a known location that easier to locate relevant data in response to an e-discovery request quickly.

10) **Data location**

In cloud computing, the data is stored in different distributed boundaries to data centers. The proposed framework overcome this challenge due to all data stored in a single data center where being discoverable, thus making it easier to retrieve that data.

5. Conclusion

This work has focused on a SaaS cloud service because it still relies wholly on CSP to collect any related data. Recently, all previous proposed works focus on certain factors to build frameworks inside a cloud location, and most of them still depend on CSP for cloud investigation. In this paper, cloud forensics investigation in any SaaS environment overcomes these challenges. It has been done by designing a framework containing a digital server located outside the cloud, and the monitoring system has captured all connections between the cloud service and the user device. A virtual cloud/organization environment was built using a VMware workstation and running different software in the implementation. Then, it used two crime case studies to evaluate and test the proposed framework. Moreover, the evaluation result has proved the feasibility of the proposed framework to collect related data that could help build proven evidence and a complete report in front of a court of law. Finally, it analyzed the results against NISTIR 8006. In future works, experiments on other cloud storage services could be performed to scale up the experiments and apply the proposed framework in a real cloud computing environment and could apply different attack scenarios.

References

[1] M Haris, RZ Khan, A systematic review on cloud computing," in International Journal of Computer Sciences and Engineering, Bikaner, Rajasthan ,India, 2018, pp. 632–639.

[2] Grand view research, Market analysis report (Cloud Computing Market Size), Grand view research, San Francisco, USA, [Online]. Available: https://www.grandviewresearch.com/industry-analysis/cloud-computingindustry.

[3] D Povar, DS Vidyadharan, KL Thomas, Digital image evidence detection based on skin tone filtering technique," in International Conference on Advances in Computing and Communications, Springer, Berlin, Heidelberg, 2011, pp. 544 551. DOI: https://doi.org/10.1007/978-3-642-22709-7_53.

[4] A Alenezi, HF Atlam, GB Wills, Experts reviews of a cloud forensic readiness framework for organizations," in Journal of Cloud Computing, SpringerOpen,2019, pp. 1–14. DOI: https://doi.org/10.1186/s13677-019-0133-z.

[5] K Ruan, J Carthy, T Kechadi, M Crosbie, "Cloud forensics," IFIP International Conference on Digital Forensics, Springer, pp. 35–46,2011.

[6] A Pichan, M Lazarescu, ST Soh, Towards a practical cloud forensics logging framework," in Journal of information security and applications, Elsevier,2018, pp. 18–28.

[7] J. Park, S. Na, J. Park, E. Huh, C. Lee and H. Kim, "A Study on Cloud Forensics and Challenges in SaaS Application Environment," 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016, pp. 734-740, doi: 10.1109/HPCCSmartCity-DSS.2016.0107.

[8] D. Birk and C. Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments," 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, 2011, pp. 1-10, doi: 10.1109/SADFE.2011.17.

[9] SA Ali, S Memon, F Sahito, "Challenges and Solutions in Cloud Forensics," Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing (ICCBDC'18). Association for Computing Machinery, New York, NY, USA, pp.,2018, pp. 6–10, doi:https://doi.org/10.1145/3264560.3264565.

[10] G. Narayana Samy, B. Shanmugam, N. Maarop, P. Magalingam, S. Perumal and S. Albakri, "Digital forensic challenges in the cloud computing environment", in Recent Trends in Information and Communication Technology, Springer, Cham ,2018, pp. 669-676, doi: 10.1007/978-3-319-59427-9_69.

[11] Ali, M.Iman and Kaur, Sukhkirandeep and Khamparia, Aditya and Gupta, Deepak and Kumar, Sachin and Khanna, Ashish and Al-Turjman, Fadi, "Security challenges and cyber forensic ecosystem in IOT driven BYOD environment", in IEEE Access, IEEE,2020, pp. 172770–172782.

[12] Ali, A.Qasem and Sultan, A.Md and Abd Ghani, A.Azim and Zulzalil, Hazura, "A systematic mapping study on the customization solutions of software as a service applications", in IEEE Access, IEEE,2019, pp. 88196–88217.

[13] S Zawoad, R Hasan, "Towards building proofs of past data possession in cloud forensics", in ASE Science Journal, Springer, Cham ,2012, pp.195– 207.

[14] ME Alex, R Kishore, "Forensics framework for cloud computing", in Computers & Electrical Engineering, Elsevier ,2017, pp. 193–205, doi: https://doi.org/10.1016/j.compeleceng.2017.02.006.

[15] Daryabar, F., Dehghantanha, A., & Choo, K. K. R. , "Cloud storage forensics: MEGA as a case study", in Australian Journal of Forensic Sciences, Taylor & Francis ,2017, pp. 344–357, doi: https://doi.org/10.1080/00450618.2016.1153714.

[16] MNA Khan, SW Ullah , "A log aggregation forensic analysis framework for cloud computing environments", in Computer Fraud & Security, Elsevier ,2017, pp. 11–16, doi: https://doi.org/10.1016/S1361-3723(17)30060-X.

[17] Herman, M., Iorga, M., Salim, A. M., Jackson, R. H., Hurst, M. R., Leo, R., Lee, R., Landreville, N. M., Mishra, A. K., Wang, Y. et al. in Nist cloud computing forensic science challenges', National Institute of Standards and Technology, 2020, pp. 10–70.

Arwa AL-Mohammdi is has a master's degree from the Information Technology Department with the Faculty of Computing and Information Technology, King Abdulaziz University (KAU), Jeddah, Saudi Arabia. She has a broad interest in cloud computing, digital forensics, IoT, and information security.

Nermin Hamza is currently Assistance Professor at faculty of grduate studies for statistical research, Cairo University. Her research interests include network security, information security, cloud security, no-SQL databases and big data areas. She worked Assistance Professor at King Abdulaziz Universit.

Shireen Saifuddin is currently an Assistant Professor with the Information Technology Department with the Faculty of Computing and Information Technology, King Abdulaziz University (KAU), Jeddah, Saudi Arabia. She has broad interest in educational technologies, information security and privacy in general, and software engineering.

Appendix A

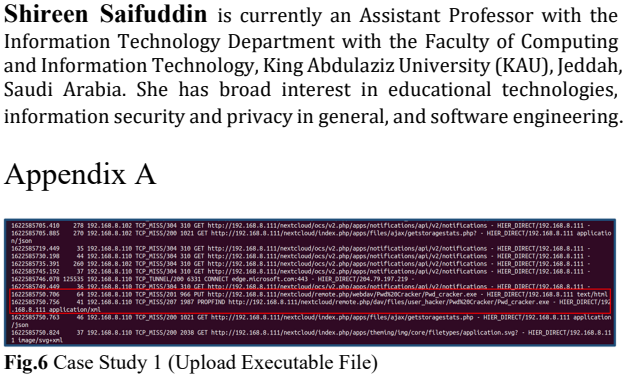

Fig.6 Case Study 1 (Upload Executable File)

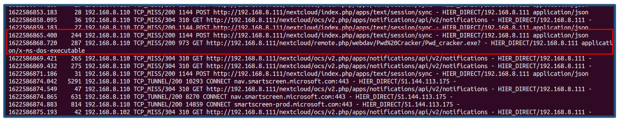

Fig.7 Case Study 1 (Deals with executable file 1)

Fig.8 Case Study 1 (Upload XML file 1)

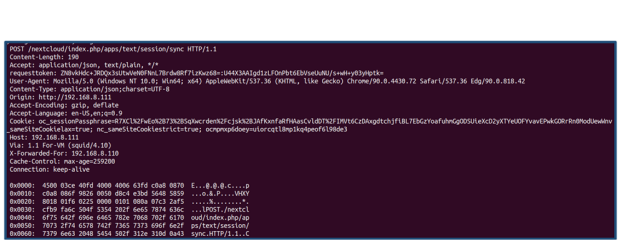

Fig.9 Case Study 1 (Logout)

Fig.10 Case Study 1 (Client Side)

Fig.11 Case Study2 (Upload Photos)

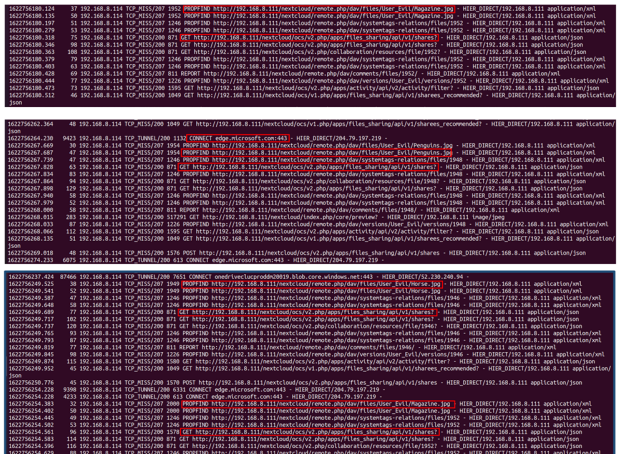

Fig.12 Case Study 2 (Share Photos)

Fig.13 Case Study 2 (Delete Photos)

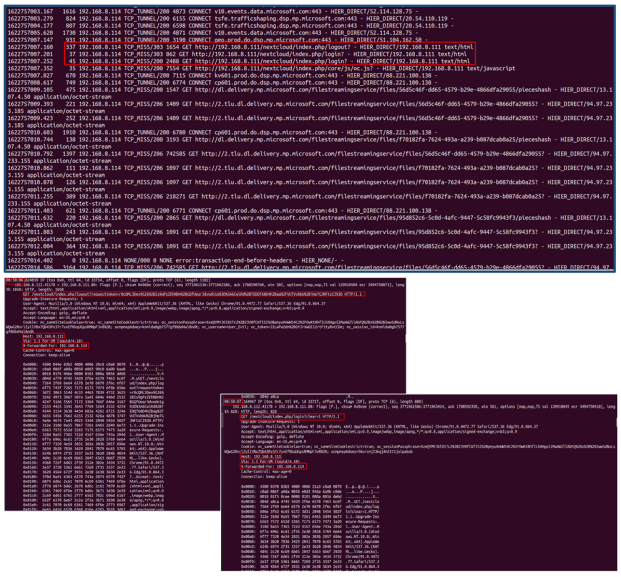

Fig.14 Case Study 2 (Logout)

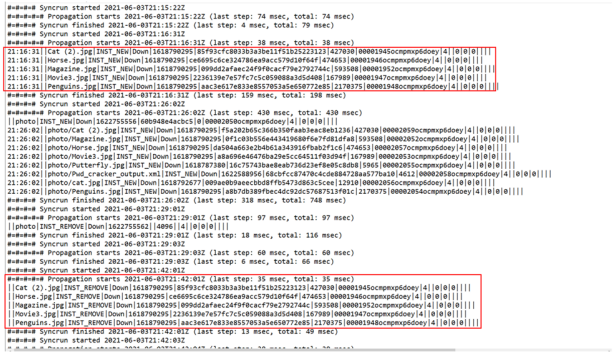

Fig.15 Case Study 2 (Client Side)