International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 12 August 2023 **Revised:** 29 September 2023 **Accepted:** 19 October 2023*

A Conceptual Cloud Forensic Investigation Process Model for Software as a Service(SaaS) Applications

Varshapriya N Jyotinagar[1], Bandu B Meshram[2]
[1]Department of Computer Engineering and IT
VJTI
Mumbai,India
varshapriyajn@ce.vjti.ac.in
[2]Department of Computer Engineering and IT
VJTI
Mumbai,India
bbmeshram@ce.vjti.ac.in

Abstract— This paper explore a structured and systematic approach cloud forensic investigation process model for SaaS applications, to investigate the digital crimes in the cloud environment and contributing to enhanced security and privacy of acquired data during forensic investigation .The proposed model offers the distinctive characteristics of cloud environments and the varying levels of access and control within them. In this proposed model, the systematic forensic investigation process is detailed with microscopic details with four phases namely the initial phase, the acquisition phase, the analysis phase, and the reporting phase in Cloud environment. Ultimately, this research aims to enhance the overall trustworthiness and reliability of SaaS applications forensic for fostering a safer and more secure cloud computing forensic investigation landscape by using the chain of custody.

Keywords- Database Forensics, Logs, Packet analysis, SaaS

I INTRODUCTION

Cloud computing has become an indispensable aspect of modern technology, providing users with convenient access to applications and services via the Internet. However, the increasing adoption of cloud computing by businesses and organizations has brought forth the need for robust security and data integrity measures in cloud environments. Recent times have witnessed numerous attacks targeting cloud computing services, emphasizing the significance of digital forensics within the cloud infrastructure.

In particular, the rise of Software as a Service (SaaS) applications has posed fresh chal- lenges for digital forensic investigators. The distributed nature of the cloud and the intricate dynamics among users, applications, and service providers further complicate forensic investigations in this context. These complexities demand innovative approaches and techniques to effectively address digital crimes and ensure the trustworthiness of cloud-based systems. As a result, the integration of digital forensics within cloud environments, especially for SaaS applications, has become imperative. By developing comprehensive methodologies and strategies tailored to the unique characteristics of the cloud, investigators can overcome the challenges posed by distributed infrastructures and intricate interactions. This research aims to explore and tackle these challenges, paving the way for enhanced security, integrity, and reliability of cloud computing systems.

Digital crime investigations in cloud environments pose numerous challenges for law enforcement and forensic investigators. These challenges encompass data fragmentation, as evidence is dispersed across multiple servers, complicating identification and collection efforts. Additionally, data encryption at rest by cloud providers hampers access without the requisite encryption keys. Determining data ownership proves problematic in the cloud, impeding the acquisition of search warrants for data seizure. Moreover, international jurisdictional complexities arise when cloud providers operate in different countries, hindering collaboration with foreign law enforcement agencies. Lastly, the rapid turnover of data in the cloud, with short retention periods before deletion or overwriting, adds pressure to investigators aiming to gather crucial evidence before it becomes irretrievable.

In this work, we propose a conceptual cloud forensic investigation process model for SaaS applications that addresses some of the mentioned challenges of investigating digital crimes in cloud environments. The proposed model outlines a structured and systematic approach to conducting forensic investigations in SaaS applications, taking into account the unique characteristics of cloud environments and the different levels of access and control in these environments. The model integrates existing forensic investigation processes with cloud-specific concepts and techniques to enable investigators to gather and analyze digital evidence effectively. We have divided the proposed model into four phases. These four phases are the initial phase, the acquisition phase, the analysis phase, and the reporting phase. The proposed work contributes to the development of a comprehensive framework for cloud forensic investigations in SaaS applications. The proposed model provides a foundation for developing effective investigation strategies and tools to enhance the security and privacy of cloud computing environments.

The paper is organized as follows:Section II covers the literature review, Section III talks about Proposed Cloud Forensic Investigation Model, Section IV includes Chain of Custody followed with conclusion in section IV.

II Literature Review

We have compiled a list of the most commonly used digital forensic process models and attempted to chronologically explain them in brief. Current digital forensics is based on the models developed from the year 2001. In the year 2001 to 2004, the following state-of-the-art models were proposed: Digital Forensic Research Workshop (DFRWS) In- vestigative Model Palmer et al. (2002) , Abstract Digital Forensic Model (ADFM) Reith et al. (2002) , Integrated Digital Investigation Process (IDIP) model Carrier and Spafford (2003) , Enhanced Integrated Digital Investigation Process (EIDIP) model Baryamureeba and Tushabe (2004) . Based on the shortcomings (such as a large number of steps, slow processing, etc.) of these digital forensic models further development was done in the year 2006 to 2013. These advanced proposed models were: Digital Forensic Triage Process Model (DFTPM) Rogers et al. (2006a) , Digital Forensic Model-based on the Malaysian Investiga- tion Process (DFMMIP) Perumal (2009) , Systematic Digital Forensics Investigation Model(SDFIM) Agarwal et al. (2011) , Integrated Digital Forensic Process Model and Triage Model (IDFPMTM) Rogers et al. (2006b); Kohn et al. (2013) . Some of these models were designed for data acquisition model and they were time sensitive. In our proposed model we tried to remove the time dependency by using disk imaging and maintaining integrity using hashing security. These models were also having issues such as a lack of transparency, virtualization, legal issues, etc.

Trenwith et al. (2013) proposed a model that, considers centralized logging of all activities of all the participants within the cloud in preparation for an investigation Trenwith and Venter (2013) . But it is causing privacy issues. To overcome this issue we decided to take logs only from machines that were attacked, that too with the consent of the owner. Alluri et al. (2015) proposed a framework for the introspection of virtual machines Alluri and Geethakumari (2015) . Their work requires a cloud multi-tenant environment. Nanda et al. (2016) Nanda and Hansen (2016) proposed a multi-tier cloud architecture for Forensics- as-a-Service (FaaS) capable of handling the aforementioned challenges and introducing new infrastructure-level forensic support from cloud providers. Their investigation model also required multiple servers. In this proposed approach we avoided the multiple servers by taking logs into a single machine and then processing it.

Most of these reported models were single-machine multiple application types. but nowa- days there is a need for a model that works with cloud services as well. Cloud services are provided by service providers, where data security is a major concern for the client. An attempt to provide a possible solution for cloud services attacks was proposed by Manoj et al. (2016) Manoj and Bhaskari (2016) along with exposure to various issues related to data security in the cloud. They also explored various challenges faced by forensic experts in the cloud. Further Battistoni et al. (2016) Battistoni et al. (2016) discussed the collected results, showing the effectiveness of data security in the cloud. Alex et al. (2017) Alex and Kishore (2017) highlighted different challenges faced by these approaches when forensic investigators are trying to work with the cloud. Du et al. (2017) proposed four step solution to these challenges: Acquisition, Identification, Evaluation, and Admission. Simou et al. (2018) Simou et al. (2019) presented a methodology that aims on assisting designers to design cloud forensic-enabled services with these 4 step solutions. But their proposed method was not consumer-oriented. Moussa et al. (2019) proposed a consumer-oriented cloud forensic process model. As a result, a cloud forensic process model that takes consumer perspective into account has been proposed. Khanaf seh et al. (2019) presented a comprehensive survey highlighting issues with these various frameworks and their solutions in digital forensics, with a focus on consumer- oriented cloud forensics. All these cloud-based solutions were highly dependent on public cloud service providers (CSP). Hence in our proposed approach, we limited our study to private cloud service providers only. Khan et al. (2020) Khan and Varma (2020) introduce an innovative solution that integrates accessing the virtual hard disk from the cloud envi- ronment at any given time with no requirement to use the CSP or any alteration to the basis of the CSP. A forensic process model is proposed that considers the possibility of multiple parallel event sequences that must be considered to achieve correctness in event reconstruction in the digital forensic investigation by De et al. (2020). But their proposed approach was limited to parallel events.

Article Received: *12 August 2023* ***Revised:*** *29 September 2023* ***Accepted:*** *19 October 2023*

Sakthiven et al. (2020) Sharma et al. (2020) present a mobile cloud forensic process framework with the help of UML diagrams that primarily consists of identification, collection, preservation, examination, analysis, evi- dence correlation, and presentation phases. Their work has two major drawbacks i.e. lower computational capability due to the mobile environment and large number of phases for digital investigation. Hence in our proposed model, we decided to limit the model to 4 phases only. Ariffin et al. (2021) aim to provide indicators for Digital Forensic organizations' maturity and readiness in the era of industrial standard 4.0 Ariffin and Ahmad (2021) .

Al-Dhaqm et al. (2021) hypothesize that the literature is saturated with ambiguities and that there is a need for a cloud forensic model that can work with SaaS applications. Maheshwari et al. (2021) propose a machine learning forensics prototype to predict fraudulent emails in advance to avoid victimization by cyber crimes. The machine learning approach was useful but needed feature extractions and hence we decided to use deep learning for our analysis phase. Das et al. (2021) proposed a model of cloud forensic application with the assurance of cloud logs. The cloud preservation and cloud log data encryption methods were mostly implemented in Python. Hence we also decided to propose a Phyton-based implementation of the proposed digital forensic model. Based on the state-of-the-art literature, we could find out that there is a strong need for a cloud forensic investigation process model for SaaS applications as mentioned by Al-Dhaqm.

III PROPOSED CLOUD FORENSIC INVESTIGATION MODEL

The process of investigating digital evidence in a cloud environment can be described as a cloud surface forensic investigation process. One such proposed cloud surface forensic investigation is shown in figure 1.

As shown in figure 1, the proposed model involves collecting and extracting evidence from both the private cloud service provider (CSP) and cloud users (CU) to reconstruct a complete timeline of a crime or incident. To implement the proposed process, digital investigators must follow a systematic approach, that involves recovering various types of data files from compromised software applications running on servers hosted on the private cloud. The investigation process includes identifying deleted, suitable, and destructive files. Then sorting them according to their types, and comparing their hashed values with the NIST database's hash list.

This manuscript introduces an optimized workflow for conducting forensic investigations in cloud environments. We are proposing a novel digital investigation process considering all the points mentioned above. Our proposed model is divided into 4 phases. In following subsection, we will explain each of the 4 phases.

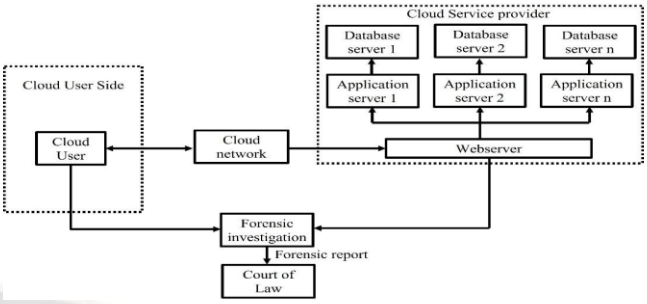

Figure 1: Cloud surface for forensic investigation

3.1. Initial phase

The Fig. 2 shows initial phase of the proposed model. The proposed methodology involves two sets of teams: a forensic team and a target-side team representing the cloud service provider. The first step for the forensic team is to select a suitable investigation tool. The investigator will take the permission for the investigation of cloud computing system and decide the probable investigation team and tools required for the forensic.

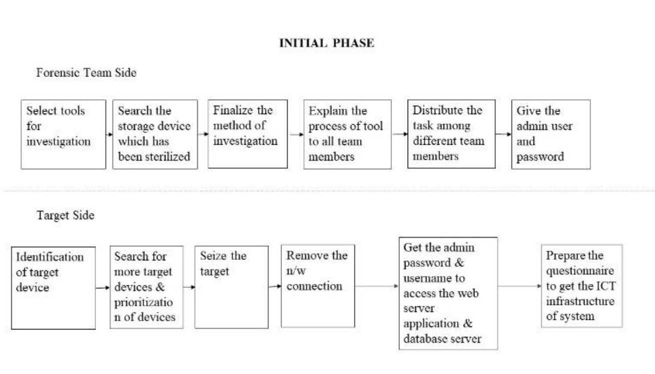
INITIAL PHASE
Forensic Team Side
Select tools for investigation
Search the storage device which has been sterilized
Finalize the method of investigation
Explain the process of tool to all team members
Distribute the task among different team members
Give the admin user and password
Target Side
Identification of target device
Search for more target devices & prioritizatio n of devices
Seize the target
Remove the n/w connection
Get the admin password & username to access the web server application & database server
Prepare the questionnaire to get the ICT infrastructure of system

Figure 2: Proposed Model of Initial Phase

from options such as Encase, FTK, and Frost. In this case, the Frost tool is chosen since it is open source. Once the tool is determined, the forensic team proceeds to locate a sterilized device capable of securely storing the virtual machine (VM) image.

The investigation method must include assigning responsibilities for capturing the system image and specifying the image acquisition process. The next step involves providing comprehensive tool usage instructions to all team members.

Subsequently, the tasks related to the investigation are distributed among the team members, ensuring clarity regarding individual responsibilities. Additionally, the team members requiring access to the affected machine should obtain the necessary usernames and pass- words provided by

***Article Received:** 12 August 2023 **Revised:** 29 September 2023 **Accepted:** 19 October 2023*

the target team.

Moving on to the target-side team, their initial tasks involve identifying the target de- vice(s) and prioritizing them if multiple devices are involved. Once identified, the target devices are seized, and their network connections are removed to prevent unauthorized data retrieval or deletion. The administrative credentials for accessing the application server and database server are shared with the investigator.

Concluding the initial phase, a questionnaire is created for the affected system users to gather valuable information about the infrastructure at the target site**.**

3.2. Acquisition Phase

Figure 3 shows the block diagram of proposed model's acquisition phase. Prior to acquiring the image, it is advisable to initiate a search for deleted files. These files of significance, encompass the log files of the web server, application server, and database server.

1.The acquisition phase involves gathering data from the identified sources in the initial phase. To achieve this, we capture an image of the compromised system that houses the web server (WS), application server (AS), and database server (DS), while also generating a hash of the image. This image is then stored on a sanitized and sterilized disk. Subsequently, another hash is generated and compared to the initial hash to ensure that both the image on the sanitized disk and the original data of the compromised system are identical.

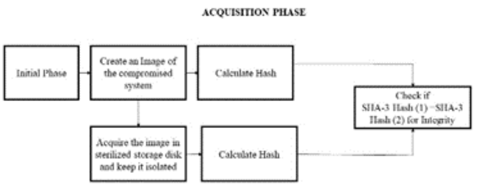
ACQUISITION PHASE
Initial Phase
Create an Image of the compromised system
Calculate Hash
Check if SHA-3 Hash (1) =SHA-3 Hash (2) for Integrity
Acquire the image in sterilized storage disk and keep it isolated
Calculate Hash

Figure 3: Proposed model acquisition phase

2 The specific type of image utilized depends on the tool employed. Typically, formats such as RAW, SMART, AFF, and E01 are employed for saving the image.

3. During the investigation, it is crucial for the investigator to recover the deleted files from the following locations: the path of web server logs, the path for catalina log, localhost log, and access log files located in the tomcat_base_dir/logs directory. Additionally, the investigator should explore the path of application server logs, localhost log, and localhost access log files as well as the path of database server logs
4. The tools used in acquisition phase from the components of SaaS cloud environments are
5. X-Ways Forensics for Disk image and files system imaging. It is a component-based forensic software platform that can be used to create disk images and file system images of SaaS cloud environments. It can also be used to extract artifacts from OS memory, registry, processes, devices, and web browsers. The second tool is Kumodd Cloud Data Imager. It is a cloud storage forensic tool that can be used to remotely acquire cloud storage data. It has two main features: directory browsing and logical copy of selected folder tree. The third tool is Oxygen Forensics Detective. It is an all-in-one forensic software platform that can be used for mobile, IoT devices, device backups, and cloud services. It can extract a vast range of artifacts from Windows, mac OS, and Linux machines. It can also collect history of text searches, visited pages, voice-search recordings, and translations from Google web history. It can also view text searches conducted with Chrome and Safari on iOS devices backed up in iCloud.

All of these tools can be used to backup, recover, and forensically examine SaaS cloud environments. However, they have different strengths and weaknesses. X-Ways Forensics is a powerful and comprehensive forensic tool, but it can be complex to use. Kumodd and Oxygen forensic tool can be used but it will depend on the specific needs and requirements

3.3 Analysis phase

Figure 4 shows the analysis phase. Once an acquired image is verified, we can extract the data from the target system related to the application, database, and Web server. The analysis phase figure shows that the files or log files must be extracted from the image of the application server, web server, and database server. This is because data resides in different files and paths for the webserver, application server, and database server. Logging into databases is more difficult than logging in to operating systems. Web servers might have WS log files, Server side scripts, and 3rd party (installed software) files. For the Application server possible files that could be present is AS log file, System error log files, system output log files, and trace log files. For the database server, the possible files are control files, online redo files, a set of temp files, and user-created data files. Once all these files are extracted then we take log details of various events from the files. These log files are evaluated for anomalies. The last part of the analysis phase is to create a timeline of events through analysis.

***Article Received:** 12 August 2023 **Revised:** 29 September 2023 **Accepted:** 19 October 2023*

The Table 1 enlists the forensic objects of SaaS components from where probable evidence is collected and analyzed.

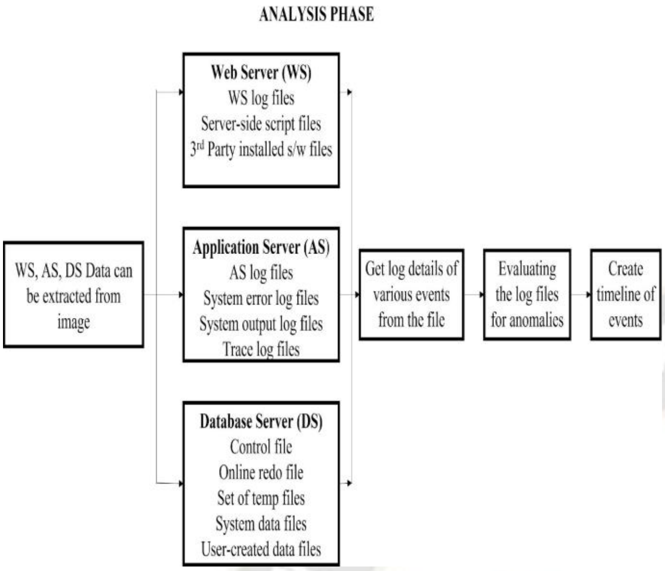

Figure 4: Proposed Analysis Phase.

3.4. Reporting phase

Figure 5 shows reporting phase of the proposed model. In the reporting phase, all the analysis and time point events in the analysis phase are considered. This is the final phase of the forensic process, and it involves writing a report that documents the findings of the investigation based on 5 W (who, where, when, what and why) and 1 H(How) analysis. The investigator use the answers to these questions to develop a timeline of events and to identify potential, relevant evidence and findings as well as any conclusions or recommendations.

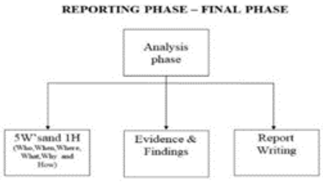
REPORTING PHASE – FINAL PHASE
Analysis phase
5W'sand 1H (Who,When,Where, What,Why and How)
Evidence & Findings
Report Writing

Figure 5: Proposed model reporting phase

A report of analysis is presented highlighting anomalies and detailed overview of the case and summary. Finally, evidence found are reported and all the findings are also mentioned. A document is prepared as per law.

IV. Chain of Custody

The chain of custody serves to demonstrate that the exhibit is likely genuine and has not been tampered with. Table 2 presents the chain of custody followed in this process model, including steps such as preparing the storage media, backing up relevant data, and seizing the target while capturing log files from the Web Server, Application Server, and Database Server.

Phases	*Activity*	*Chain of Custody*	*Output of Phases.*
Initial Phase	The initial phase starts when the forensic investigator prepares the groundwork for the forensic investigating team and target side by identifying the target location, identification of hardware and software tools.	The chain of custody process involves identifying, labelling, and recording the SaaS system.Visit the incident scene. Then, the network connection is removed, and Target is seized.	Planning, Authorization, Warrant, Investigation permission,
Acquisition and Preservation Phase	Recover deleted data and back up. Capture screenshots throughout the process and the acquired data may be hashed, compressed, encrypted and digitally signed and packed in Signal Blocking Bag.	The investigator team will retrieve various log files from the Web server, Application server, and Database Server and administrator acquire the image and verify the hash of the image before and after acquiring. One can preserve the imaging and cloned data for Confidentiality, Integrity and authenticity of the forensic information.	Imaging data and cloning with all objects. Digital certificate for preservation in digital forensic laboratory for security and safety.
Examination and Analysis Phase	The extracted data can be analyzed using standard processes and tools from the acquired image and cloning.	Digital forensic Investigator team, For example cybercrime police, domain expert	Log files, Event Log, Metadata, Path of potential evidence
Reporting Phase	Prepare the forensic report	Reporting includes the following: 1)Summary of Case and Task. 2)Summary of Compliance 3)Forensic examination of Hardware and Software Tools used. Statement regarding Chain of Custody	Forensic report and its documentation.

Article Received: *12 August 2023* ***Revised:*** *29 September 2023* ***Accepted:*** *19 October 2023*

Phases	***Activity***	***Chain of Custody***	***Output of Phases.***
		for access control and security. Evidence Analysis and Classes of Evidence 4)Summary of Conclusion reached Expert Opinion regarding the findings.	

Table 2: Proposed Chain of Custody.

Cloud Component	**Forensic Objects**
Web Server	Catalina.log,Catalina.out,localhost_access_log.txt, localhost.log ,manager.log, error logs, audit logs, security logs and Network captures like pcap, tcpdumps may also be analysed.
Application Server	localhost_access_log.txt, localhost.log
Database Server	Data files, Control files, Online redo log files, archived redo log files, Tablespaces, Alert log files, Background trace files, Foreground trace files, Initialization parameter files, audit trail files, Incident log files, TNS listener log files, virtual tables

CONCLUSION

The proposed model has been designed and focuses on the initial phase, which deals with preparation for incident response at the client and target side. Additionally, the model consists of the acquisition phase, which involves acquiring the image of the victim's or compromised system in the private cloud by visiting the data center through the information collected in the initial phase. The model also includes an analysis phase that extracts data from the relative path of the application server and database server using existing and newly designed tools. Furthermore, the proposed model includes a stepwise chain of custody, The final stage of the proposed model is the reporting phase, which presents the forensic investigation process in documentation format. Overall, the proposed model offers a comprehensive and well-structured approach to cloud forensic investigation, which can significantly improve the effectiveness of the incident response process for SaaS.

Future work includes testing the proposed model on a SaaS application deployed on a private cloud, as well as developing a tool that can extract data from the relevant path out- lined

REFERENCES

[1] Agarwal, A. Gupta,M., Gupta,S., Gupta,S.C.. Systematic digital forensic investigation model.International Journal of Computer Science and Security (IJCSS) 2011.

[2] Al-Dhaqm, A., Razak, S., Ikuesan, R.A., Kebande, V.R., Othman, S.H.. Face validation of database forensic investigation metamodel. Infrastructures 2021.

[3] Alex, M.E., Kishore, R.. Forensics framework for cloud computing. Computers &amp; Electrical Engi- neering 2017.

[4] Alluri, B.K.R., Geethakumari, G.. A digital forensic model for introspection of virtual machines in cloud computing. In: 2015 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES) 2015.

[5] Ariffin, K.A.Z., Ahmad, F.H.. Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. Computers &amp; Security 2021.

[6] Baryamureeba, V., Tushabe, F.. The enhanced digital investigation process model. Digital Investigation 2004.

[7] Battistoni, R., Pietro, R.D., Lombardi, F.. CURE—Towards enforcing a reliable timeline for cloud forensics: Model, architecture, and experiments. Computer Communications 2016.

[8] Carrier, B., Spafford, E.H.. Getting physical with the digital investigation process. International Journal of digital evidence 2003.

[9] Das, M.S., Govardhan, A., Doddapaneni, V.L.. A Model of Cloud Forensic Application With Assurance of Cloud Log. International Journal of Digital Crime and Forensics (IJDCF) 2021.

[10] De, S., Barik, M.S., Banerjee, I.. A Digital Forensic Process Model for Cloud Computing. In: 2020 IEEE Calcutta Conference (CALCON). 2020.

[11] Du, X., Le-Khac, N.A., Scanlon, M.. Evaluation of digital forensic process models with respect to digital forensics as a service. arXiv preprint arXiv:170801730 2017.

[12] Khan, Y., Varma, S.. An efficient cloud forensic approach for IaaS, SaaS and PaaS model. In: 2nd International Conference on Data, Engineering and Applications (IDEA). 2020.

[13] Khanafseh, M., Qatawneh, M., Almobaideen, W.. A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics. International Journal of Advanced Computer Science and Applications 2019.

[14] Kohn, M.D., Eloff, M.M., Eloff, J.H.. Integrated digital forensic process model. Computers &amp; Security 2013.

[15] Maheshwari, S., Sharma, N.. Cyber forensic: A new approach to combat cyber crime1, 2. International Journal of Computer Network and Information Security 2021.

[16] Manoj, S.K.A., Bhaskari, D.L.. Cloud forensics-a framework for investigating cyber attacks in cloud environment. Procedia Computer Science 2016.

[17] Moussa, A.N., Ithnin, N., Almolhis, N., Zainal, A.. A consumer-oriented cloud forensic process model. In: 2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC). 2019.

[18] Nanda, S., Hansen, R.A.. Forensics as a service: Three-tier architecture for cloud based forensic analysis. In: 2016 15th

International Symposium on Parallel and Distributed Computing (ISPDC). 2016.

[19] Palmer, G.L,Scientist, I., View the digital world. International, H. Forensic analysis in Journal of Digital Evidence 2002.

[20] Perumal, S.. Digital forensic model based on Malaysian investigation process. International Journal of Computer Science and Network Security 2009.

[21] Reith, M., Carr, C., Gunsch, G.. An examination of digital forensic models. International Journal of digital evidence 2002.

[22] Sharma, P., Arora, D., Sakthivel, T.. UML-based process model for mobile cloud forensic applica- tion framework-a preliminary study,International Journal of Electronic Security and Digital Forensics 2020.

[23] Simou, S., Kalloniatis, C., Gritzalis, S., Katos, V.. A framework for designing cloud forensic-enabled services (CFeS). Requirements Engineering 2019.

[24] Trenwith, P.M., Venter, H.S.. Digital forensic readiness in the cloud. In: 2013 Information Security for South Africa. 2013.