Innovative Computing Review (ICR)
Volume 1 Issue 2, Fall 2021
ISSN$_{(P)}$: 2791-0024 ISSN$_{(E)}$: 2791-0032
Journal DOI: https://doi.org/10.32350/icr
Issue DOI: https://doi.org/10.32350/icr/0102
Homepage: https://journals.umt.edu.pk/index.php/icr

Article: **Cloud Forensics: Challenges and Solutions (Blockchain Based Solutions)**

Author(s): Hassan Kaleem

Affiliation: KIT Cloud Solutions Limited, London, United Kingdom

Citation: K, Hassan, "Cloud Forensics: Challenges and Solutions (Blockchain Based Solutions)", *Innova Comput Rev*, vol. 1, no. 2, pp. 01–26, 2021. https://doi.org/10.32350/icr/0102/01

Journal QR

Article QR

Hassan Kaleem

A publication of the
School of Systems and Technology
University of Management and Technology, Lahore, Pakistan

Cloud Forensics: Challenges and Solutions (Blockchain Based Solutions)

Hassan Kaleem[1]*, Ijaz Ahmed[2]

ABSTRACT: Cloud computing is an on-demand service provided for computer resources, data storage and enhancing computing power. Digital forensics is used to help forensic investigators extract evidence against cloud/ cybercriminals and maintain the integrity and security of data stored in a cloud environment. Based on the prior research in this area concerning existing challenges and solutions, this survey focuses on exploring the problems and their proposed solutions on the basis of a detailed literature survey. It critically explores and reviews the prevailing challenges and solutions through an in-depth review of the cloud forensic area. The paper highlights all the current problems in cloud forensics and their solutions previously identified by the researchers to help investigators probe any criminal incident. The three categorization model explores the challenges and solutions of the existing methods and offers directions for future research in this area. Finally, this survey paper can be considered an initiative to carry out research and develop cloud forensic-able services for the cloud environment.

INDEX TERMS: blockchain based solution, cloud forensics, cloud forensics challenges, cloud forensics methodologies, cloud forensics solutions

I. INTRODUCTION

Cloud computing is currently the most important topic which is fast gaining popularity in the information technology sector because firms are moving from traditional systems to cloud computing. After all, it is economical, reliable, and on-demand. According to Forbes contributors, cloud computing has gained ground over and above its 30% ratio. The International Data Corporation had predicted that by the year 2021, firms spending on

[1] KIT Cloud Solutions Limited, London, United Kingdom
*Corresponding Author: hassanrao.hr@gmail.com

software and hardware to help cloud services, will cross their 59% IT budget mark [1]. Many industries are daily abandoning their traditional system for cloud computing. A considerable number of companies too are following the suit. It is well known that the moment you put your data online it is under constant threat because people, data, and money do attract crime. According to McAfee's global cyber work report [2] (including cloud crime), it (cloud crime) costs $ 500 billion each year. The main purpose of this article is to provide a comprehensive review of tools and methods that interact with or assist in cloud forensic. The paper reviewed its challenges to and solutions for cloud forensics on the basis of detailed field reviews. The work revolves around both cloud and digital forensics (cloud forensic being subset of digital forensics).This research also includes the efforts needed to be made in this area, and the tools required to be implemented to assist the cybercrime investigations in the cloud environment. According to the National Institute of Standards and Technologies (NIST) there are 65 [3] forensics science problems in cloud computing. As many as 20 major problems and solutions have been in this paper. The paper has been organized in the following sections: First, it provides all the methodologies for digital and cloud forensics. Secondly, it reviewed the algorithms and tools developed to facilitate forensic investigation and finally the legal requirements issues needed to be tackled to make a strong case for the court of law. The first part concludes that there are four steps in any digital or cloud forensics. They are: Identify, preserve, extract and present. Identification is the first stage in which one has to collect all the evidence from the cloud environment. It is the most difficult part of the investigation due to the geographical distribution of the system, usage of the same network by many users, and the processing speed. To prove that the incident has occurred, c loud forensic investigator needs to identify its type and the assets which were used (software, and hardware). They also need to identify the cloud provider and data centers. After that, a team of cloud forensics investigators is formed. It comprises people of different skills sets suitable for cloud environment such as experienced officers, legal advisors, and law personnel. In the identification stage, a warrant for search to access those CSP's infrastructure has to be issued. All the actions taken to identify the valid evidence and to notify methods and people used to investigate the crime, need to be properly recorded and documented. After identification, the evidence is acquired from the desired locations where it is stored in the cloud environment. Cloud forensics investigators need to separate digital evidence, disallowing unauthorized people to use the digital devices in which the incident occurred or even to duplicate the digital evidence so that it is not used against the company. This requires the services of well-trained personnel. The Analysis stage involves, extraction of the evidence from the identification and preserving stage and checking the amount of the identified data. Well-trained personnel who are adept at in the tech techniques concerned are required to examine data and extract evidence. The cloud forensics investigators who are inspecting the incident should have a high level of overview of the terrain. Otherwise, it may invite delays. They should review the stages of the previously encountered cases and the plan to identify different mechanism that can help them reduce durationof the examination. Presentation is the last stage wherein the case is presented in the court of law. One may lose a case because of even a single and minor mistake. That is why a well-documented report is needed to be created in consultation with the experts concerned to avoid any such happening. he case pleading officer should be well versed in all the relevant legal intricacies so as to prepare a strong case. Reports should be prepared with the help of the the official who fully knows the legal procedure required for such work. The report must clearly communicate in plain terms the technicalities of the information technology to the judiciary who may not know the subject. The report and its supporting material such as the chain of evidence should be presented and submitted to the court. Details of the crime such as the type of cloud incident, who is involved, and other facts like compromised accounts should be attached to it and submitted in the court.

II. RELATED WORK

The papers we have reviewed have discussed cloud forensic problems and solutions. They state that there are four basic steps in a digital forensics environment which are: Identify, preserve, extract and present. This forensic model was developed by McKemmish [4] and is mostly followed worldwide. Every day many companies are trying to move from traditional systems to cloud environments. But, still, they are concerned about their security and privacy because of the ever rising number of digital crime. A cloud security alliance survey with more than 200 IT and cyber security professionals from all over the world shows that the companies are willing to pay a huge amount of money to penetration testers to prevent a cyber-attack. More than 15.00% of the companies are willing to pay up to 1M $. The major issues in a cloud environment are the policies and regulations that should be developed to provide for a secure mechanism to protect people against hacking. Forensics is meant for dealing with these issues. For example, if you are using SAAS or PAAS, you cannot create an image of the system. But in infrastructure, as a service (IAAS), you can create the image file of the system. In a cloud environment, the crime investigator has to deal with several issues as compared to the computer or network investigator. Some of the problems are that evidence can be stored anywhere in the world. There are other issues including dependence on cloud service providers, multi-tenancy, and jurisdiction that has made this system even more complexed. Different cloud forensics techniques are developed and used in different cloud models like in PAAS and SAAS. You have to request your CSP for the log files of the system. You can create the image file in IAAS and recover the needed logs files through that. CSPs do not provide you the log files because many users are using the same processing and network. Another problem is that you cannot access physical data, like for example, hosting a website on Godaddy.com. Therefore, it is impossible to seize that storage device because it is also being used by multiple users of Godaddy.com simultaneously. Another major problem is the dependency on CSPs, which, in turn, are reluctant to provide you the evidence for the good reason that this can be misused to damage their reputation. There are other problems as well like service level agreement, client-side identification and the collection stage multi-tenancy, chain of custody, imaging, bandwidth limitations, multi-jurisdiction distribution, and collaboration. Lack of forensics tools in the test section, data volume, encryption, time synchronization, and integration of log formats are some other issues. The final difficult task stage is the submission of evidence in the court. The forensics analyst's job is to ensure that the evidence he or she possesses has been s collected through legal means and software. The analysts must carefully maintain a chain of custody to ensure victory in the court of law. The problem in the presentation section is the complexity of the evidence and all the technical details which are generally foreign to the judge and other officials because of their likely mere basic computer knowledge. presented are almost impossible to comprehend in a courtroom where a judge is made up of people with just basic computer knowledge. Therefore, all the processes used and the evidence gathered need to be explained thoroughly. Coming to the solutions this paper has presented in the identification stage, the problem is the gathering of the log files because of the lack of control of the consumer and the investigator over the CSP's Infrastructure. Many researchers have attempted to solve this issue. Zawoad has developed a secure-logging-as-a-service (SECLaaS) which keeps the logs of the virtual machine and gives access to the cloud forensics investigator while maintaining privacy of the cloud users. A live investigation can resolve the issue of volatile data. All the problems and solutions that this paper has discussed are about securing the cloud environment so that companies can move from the costly traditional system to a cloud environment that is affordable as this does not require them to pay for hardware and its maintenance . Forensics is all about locating who was the unauthorized user who hacked into your system, stole your information and used it against you. One of the main reasons why cloud service providers do not share information demanded by investigators is their apprehension that this information can be used against them. According to SC magazine, a company named Code Spaces, a former SAAS provider, is one of the 60% of the small businesses that failed within 6 months after being hacked [5].

III. RESEARCH METHODOLOGY (SYSTEMATIC LITERATURE REVIEW)

A systematic literature review has been conducted for this paper as a search methodology. The goal of this research is to provide a review of the existing problems and their solutions for cloud forensics. We have followed the methodology of a survey formed by various researchers. The research methodology for this systematic mapping study has been shown in this figure.

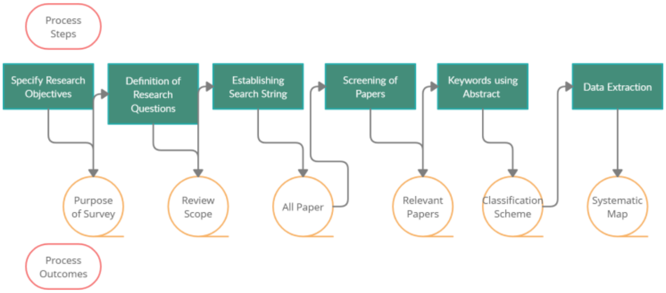

Fig. 1. Research Methodology

A. Research Objectives

This research comprised the following objectives.

O1:Identifying problems and solutions in the field of cloud forensics.

O2:Characterizing the existing cloud forensics challenges and solutions.

O3:Proposing a statement that further highlights the adopted cloud forensics methods and approaches.

O4:Proposing a cloud forensics-based smart framing framework to help spot the prevailing cloud forensics solutions.

O5:Identifying research gaps in cloud forensics challenges and solutions.

TABLE 1

RESEARCH QUESTIONS

No	Research Questions
1	What are forensics issues SaaS?
2	What are forensics issues PaaS?
3	What are forensics issues IaaS?
4	What are the issues in the identification of evidence in a cloud environment?
5	What are the issues in preserving evidence in a cloud environment?
6	What are the issues in extracting evidence in a cloud environment?
7	What are the issues in analyzing evidence in a cloud environment?
8	What are the issues in the presentation of evidence in a cloud environment? (Cross Border Legislation).

B. Search String

The second phase of this systematic literature review is to look for relevant studies on cloud forensics. An enquiry string has been defined to gather all the published papers on cloud forensics. A pilot-based search strategy has been applied to specific keywords that are associated with this study's topics. Internet search has been conducted on cloud forensics using multiple search engines and digital libraries to gather relevant information about cloud forensics. To ensure the simplest source of knowledge about cloud forensics, all the results were compiled manually. The selected search engines and digital libraries are supported by their scientific content. The selected databases include IEEE, Springer, and Reasearch Gate.

TABLE 2

Sources	Search String	Context
IEEE, Springer, ResearchGate.	Cloud forensics, cloud forensics methodology, cloud forensics challenges and cloud forensics solution	Cloud

IV. Screening of Relevant Papers

All the papers collected for this study were purely related to cloud forensics. To single out only the most relevant papers, the inquiry process defined by researchers Dyba and Dingsoyr [6] was used. In the first phase of the screening, papers related to our topics were gathered on the basis of their titles, excluding studies not related to cloud forensics. Furthermore, the exclusion and inclusion criteria were used as follows.

- Papers that were published other than technical reports, patents, conferences, and journals.
- Articles without defining data sources and the procedure for collection of data.
- Articles that were not published in the English language.
- Papers that were published before 2011.
- Papers that were not relevant to cloud forensics.

All the papers have been included and excluded on this basis. After going through their abstracts in the first phase of screening, these researchers picked these papers in the next phase of screening.

A. Keywords using Abstract

To find relevant papers relating to the topic through keywords by using the paper's abstract, we used a technique that was designed by Paterson. In the first phase, we studied the abstract of papers and identified their concepts, including keywords on cloud forensics that reflected the contribution on study. In the second phase, we developed a better understanding on the basis of the idea of these papers.

B. Quality Assessment

In a systematic literature review (SLR) quality assessment is administered to check the standard of the relevant papers.

- The study contributed to cloud forensics. The answer to the present research was Yes 1 No 0.
- The study represents a transparent solution within the field of cloud forensics. The possible answers for cloud forensics are Yes 1, purposed or partly covers the question 0.5, and No 0.
- To measure the Quality Assessment, it will be seen whether this paper has provided answers to our questions and has this paper been cited by other researchers, Yes 1 if the citation count is quite five, partially +1 if the citation count is between 1 to 5, 1 if the citation count is 0.
- The published research article is from a recognized publication source. The solution to the present question about cloud forensics has been evaluated by JCR lists and the core ranking of IT/CS conferences.

Possible answers for conferences and journals are presented in Table 2.

TABLE 3

QUALITY CRITERIA. JCR: JOURNAL CITATION REPORTS

Sources of Papers	Ranking of Question	Score
Journals	Question 1	1
	Question 2	1
	Question3	1
	Q4, Q5, Q6 and Q7	1
	If the paper is not in Journal Citation Reports Ranking	0
Conferences	X	1.5
	Y	1
	Z	0.5
	If the paper is not in Journal Citation Reports Ranking.	0

Selected research papers have a score for every question they have answered. And the sum of scores is presented in an integer value that starts from 1 to 5.

C. Selection of Result

Analysis of cloud forensics problems and solution is difficult due to the fact that it covers a lot of problems in all the three models of cloud (SaaS, PaaS and IaaS). According to our research purpose, we have collected 64 studies. After studying the gathered papers in detail we have addressed each of the questions.

D. Data Extraction Method

A data extraction technique has been applied to supply the answers to the cloud forensics challenges.

RQ1:The question is solved by identifying the issues in SaaS model for cloud forensics.

RQ2:The question is solved by identifying the issues in PaaS model for cloud forensics.

RQ3:The question is solved by identifying the issues in IaaS model for cloud forensics.

RQ4:The question is solved by identifying the main issues in identification stage in cloud forensics.

RQ5:The question is solved by identifying the issues in preservation stage in cloud forensics.

RQ6:The question is solved by identifying the main issues in extraction/analysis stage in cloud forensics.

RQ7:The question is solved by identifying the main issues in presentation stage in cloud forensics.

E. Cloud Forensics Challenges

In the challenges section, we will present problems of forensics in a cloud environment through systematic literature review. These problems have been identified through reviews and research papers that were presented in cloud forensics.

V. IDENTIFICATION STAGE

A. Access to Logs

Logs play an important role in forensics investigation. In order to identify that who hacked into your system, forensics investigator’s first priority is to get access of logs files. These logs files can be collected easily when you are a computer forensics investigator. But when you are in cloud environment, you cannot easily access the logs file. In SaaS and PaaS, getting access to the logs files is difficult because the user’s access is limited. It is partly applied to IaaS but many CSPs do not gather logs or they try to hide these log files from users because they think they can be used against them.

B. Physical Inaccessibility

In cloud environment, getting physical access to data is impossible because the data you need is on different geographical locations. The forensics tools that are developed for investigations need physical access of the system. But in the cloud environment, the data you need is on a hardware device and that is on another geographical location, and is being used by multiple users simultaneously. This makes it impossible to seize that hardware device.

C. Volatile Data

Getting access to the volatile memory (capturing RAM, temporary file, and tabs) is mandatory for a forensics investigator. Because once hardware loses power, the potential evidence is lost.

D. Client Side Identification

Collecting evidence from user's side plays an important role in forensics investigation. Sometime evidence can be found on user's side as well. In most of the cases, SaaS and PaaS user web browser is the only application that interacts with the cloud. Once the cases are reported, the forensics investigator needs to carefully collect all the evidence from client's side as soon as possible.

E. Dependence on CSPs

In cloud environment, everything is owned by the CSPs who are responsible for assisting clients in case of any incident. Problems come when CSPs do not assist clients in forensics investigations. This is so because they think it might be used against them. In SaaS and PaaS, clients are fully dependent on cloud for l help in identifying evidnce. But the cloud doesn't have certified forensics experts. And due to its transparency issues, it is hard to trust the legitimacy of the data it provides. Another problem is that CSPs use data centers on contracts whereas a forensics investigator needs to involve all the parties in order to extract e evidence.

F. Service Level Agreement

There is a lack of customer awareness and international laws regarding cloud environment. SLA should include important terms related to cloud forensics. They are responsible in case of any incident. But in most cases CSPs donot provide transparency to customers or their techniques that are currently in use but are not compatible with cloud forensics investigation or they don't know how to conduct criminal investigations. CSPs should also provide transparency. For example, if a contract between CSP and client expires according to SLA, CSP is responsible for destroying the hardware devices the clients were using, ensuring that it is not recovered. But how a client can know that CSP has destroyed the hardware device is a question that needs a proper answer.

VI. PRESERVATION STAGE

A. Integrity and Stability

The integrity and stability of the evidence is compulsory for forensics investigation. Data must be preserved without violating ny law (collected through legal ways). Losing the integrity of the evidence would mean losing the case in the court of law. In IaaS and PaaS, many users use the same storage devices and processing speed simultaneously. So forensics investigator needs to be very careful about the privacy of the users and the data he is presenting in the court of law, also ensuring that the data does not include any other user's data.

B. Internal Staffing

This internal staffing covers all service models SaaS, PaaS and IaaS, and every stage of investigation like identification, preservation, collection and presentation. To proceed with an investigation in cloud environment, one needs individuals with specialized skills for conducting a forensics investigation.

C. Chain of Custody

The final part is the presentation of the case before the court. And this is the most important and difficult part. Because the court may merely have a basic knowledge of computers and the complicated cloud environment. It is therefore important to give it a clear idea of the issue through the chain of custody. Any flaw in the chain of custody will amount to losing the case.

D. Imaging

The image of the system is captured by taking its snapshot in IaaS. But in SaaS and PaaS, the user has no control over the infrastructure. The access is also limited. Thus he cannot create the image of the system without which it is impossible to extract evidence from the storage device of the volatile memory.

E. Bandwidth Limitation

The volume of the knowledge in cloud environment is large. If you're close to taking the image of the system in IaaS model, you would like to stay in mid bandwidth limitation. This is so because you've got to download the image files so as to perform analysis.

F. Multi-Jurisdiction

Extracting evidence from cloud models like SaaS, PaaS and IaaS is another issue. Due to the geographical distribution of the data, it is impossible to conduct investigation. The court order issued for collecting the evidence may not be applicable because the data you need is on different location where another country's law is applicable. Another issue is that whose law will be applicable in deciding the case because the parties and the evidence involved are placed in different legal jurisdictions of the world.

VII. EXAMINATION AND ANALYSIS STAGE

A. Lack of Forensic Tools

Analysing your data in cloud environment requires special forensics tools, for example, Autopsy, Encase and Access Data FTK. On the contrary, the tools that are developed in forensics support other branches of digital forensics like computer forensics and mobile forensics. Complications in cloud environment like geographical distribution of data, having no access to storage devices, make it impossible to collect evidence through these software. According to a need analysis survey on cyber forensics [7], 40% of the participants involved in that survey, think that these forensics software need improvement.

B. Volume of Data

The volume of knowledge in cloud environment is very large and is counting daily. Therefore, it is real difficult to extract evidence from cloud environment and to perform analysis. In the SaaS and PaaS model it's very difficult to research the virtual machines directly. The SaaS and PaaS may have large storage because they also contain many other applications. It's very difficult albeit CSP is cooperating with you.

C. Encryption

In all the three models of cloud SaaS, PaaS and IaaS, all the users store their data in encrypted format so the criminals are unable to use it even after managing to hack into the system. To perform analysis on these encrypted files is another difficult task for forensics investigator because he has to obtain keys for the purpose. And performing analysis becomes impossible if the key of the encrypted data is destroyed.

D. Time Synchronization

It is important to extract time concerned data from all the three models of cloud, SaaS, PaaS and IaaS. But it requires a lot of hard work to get to the correct results because the data one need might be placed in different geographical locations and time zones. For example, presenting a case in a court of a country will be problematic if the related data is hacked in another country and the evidence one extracted has a different timestamp.

E. Unification of Logs Formats

Analysing data is a time consuming process especially if one has to deal with multiple logs formats and voluminous data. In a cloud environment, the unification of logs formats is a difficult task. And it makes it more difficult when we have to access huge amount of different resources.

F. Identity

In computer or mobile forensics, it's very easy to spot the persons behind the incident by simply identifying who was using that system when the incident occurred. But in cloud forensics one cannot blame a specific person for hacking the system without proper investigation.

VIII. PRESENTATION

A. Complexity of Testimony

Lastly, an investigator needs to present the case to the court where officials with mere basic computer knowledge may find cloud computing extremely complicated. Therefore, the investigators need to present the case in a way whereby the court is able to easily understand the intricacies of the subject. The entire case should be presented with clarity, explaining in simple terms and with proper documents how the evidence was collected. This is mandatory for ensuring victory.

B. Documentation

Another challenge is to properly document each process and tool involved. And, therefore, the investigation should be conducted by strictly following all the principles and standards prescribed for forensics investigations. (For example ISO standards).

IX. Challenges/ Discussion

After a thorough literature review, Table 4 has been created to assign challenges to the respective stage and service model (SaaS, PaaS, and IaaS). The table also includes the related work identified by different researchers. Among the issues is compliance issue which is not categorized in any stage or model. Companies and organizations like the banking sector, stock market and hospitals are not switching over cloud environment due to trust deficit. The National Institute of Standards and Technologies (NIST) has identified 60 issues in cloud environment and our list comprises only 20 issues in cloud including compliance. Most of the challenges that are in our list are in the NIST list as well.

Cloud Forensics Solutions

X. Identification Stage

A. Access to Logs

Getting access to logs is the most vital task in cloud forensics. Zawoad [8] purposed Secure Logging as a Service (SecLaas) for cloud forensics, which allows CSPs to store logs files of virtual machines which will later be accessed by forensics investigators. Another researcher Sang [9] purposed a model in which he reduced the complexity involved. He says that we should always store our logs files locally so that in case of any need in SaaS model, we don’t have to go to CSPs to get the access to our log files. Trenwith [10] purposed a solution in which he recommended collecting all the logs files and storing them on a remote and a central server where they are archived. Patrascu [11] introduced a framework which allows an investigator to analyze the workloads and the virtual machine. In PaaS, the customer has the full control over the prepared Application Processing Interface (API). So in PaaS, the customer can extract some system status and specific logs files of the application. Birk purposed a mechanism in which the logs files are encrypted before they are transferred to the cloud server. In that case, nobody can alter logs files in the way to cloud. In IaaS model, Dykstra recommended a cloud management plane. This system can start and stop the virtual machine enabling the investigator to download the logs files._In PaaS, Dmashenas [12] recommended preparation of an API as it can extract relevant data from cloud for a specific user.

B. Volatile Data

Live investigation should be conducted to collect volatile data. Because the moment the system is powered down volatile data is erased. To overcome this issue, Birk [13] purposed a system of frequent data synchronization. This system should be placed between virtual machines and persistent storage or a local storage. According to Zawad, [14] this purposed system by Birk does not provide any guidelines on exactly how to do this.

C. Client Side Identification

Identifying evidence at client's side is another important part of forensics investigation. For that purpose, Damshenas [12] suggested that all the logs files in client's machine should be stored. However, he did not provide any guidelines and procedure on how to do this.

D. Dependence on CSPs – Trust

In cloud environment, the client is fully dependent on CSP, which creates the problem of transparency between cloud and the customer. To overcome this issue, Haeberlen [15] purposed that cloud should store its actions in a temporarily evident logs storage readily available to customers so that they can independently audit the material.

E. Service Level Agreement (SLA)

In the cloud forensics problems session, we have discussed important terms that should be included for cloud forensics in SLAs. To overcome this issue, Ruan [16] suggested that these terms should be included in SLAs like roles and responsibilities between CSPs and the customers. A well defined and detailed SLA should be agreed upon and signed by CSPs and customers, covering the client privacy policy, Damshenas [12] and Baset [17] stated. In order to gain trust of customers, CSPs need to jot down these SLA for future contracts. These include service guarantee time period, violation detection credit, outcome based SLAs andt standardization of SLA. An SLA framework for e-commerce is purposed by Busalim [18].

F. Integrity and Stability

Validating the integrity is another important part in forensics. Any loss of integrity can cost you your case. To handle this issue, a digital signature system was introduced by Zawad [14] to repeatedly check and validate integrity of the collected evidence. A distributed signature system was developed and implemented by Hegarty [19]. This detection framework will enable the cloud forensics investigator to perform analysis on storage platform. Shi [20] presented a multi-tenancy model in SaaS, whereby the data storage issue is mapped. Zhou [21] purposed a scheme, RBE scheme, that will allow control based policies for encrypted data stored in public clouds. Yang [22] purposed data access control for cloud storage for multi -authority.

G. Internal Staffing

Conducting criminal investigation in cloud environment requires specialized personnel in order to complete the task. To overcome this issue, Ruan [16], purposed a solution which involves internal staffing of CSPs employees and special assistance from outdoor channels. The team members should be well versed in relevant laws, regulations and standards for successfully conducting investigations. The forensics investigation team should be skilled in networking, laws and regulations, negotiations with CSPs, communication and programming. Another researcher Grispos [23] purposed that CSPs should hire well-trained personnel to conduct forensics investigation in order to give their clients transparency.

H. Imaging

Taking image of the system is the most important feature of any forensics investigation and in cloud environment. Doing so in SaaS and PaaS is all the more difficult because of the users' limited access to the system. The cloud structure also prevents this. Damshenas [12] furnished a solution to this issue, suggesting collection of a diary of the system. This will help a forensics investigator create a picture of the system on the basis of the track record of the user.

I. Multi-Jurisdiction – Distribution and Collaboration

There is another problem. The data one may need is likely to be available on different geographical locations in the world. And even the court orders to collect evidence for investigation will not be binding on another country's data centers. To overcome this issue, a standard international law should be framed and implemented across the globe to facilitate forensics investigation, highlighted Ruan [16] and Sibiya [24].

J. Forensics Tools

Today the most commonly used forensics software are Encase and AccessData FTK. But these software are usable only when one has access to the hardware devices. In cloud environment, your system is geographical distributed and many users use the same storage devices, which makes it impossible to conduct investigations using these software. To overcome the privacy issue of cloud users, Juels [25] developed POR tools which guarantee other cloud users' privacy. Dykstra [26] designed and implemented a forensics tool kit for IaaS model, which is called Open-Stack Tools.

K. Volume of Data

Many users do use the same storage devices and processing network simultaneously in a cloud environment. This creates the problem of volume of data. Extracting evidence from the large image file is very difficult even if CSP is cooperating with the forensics investigators in taking image of the whole storage device. The data mining experts should resolve this issue. Kao [27] purposed a system, a model, for storing and improving the digital investigation process.

L. Encryption

Cloud stores its data in encrypted format. And decrypting it is difficult. In order to use this data, an investigator has to collect all the keys of data so as to decrypt it for extracting evidence from it. Wan [28] purposed a hierarchical attribute set based encryption system to achieve the scalability in cloud computing.

M. Time Synchronization

Due to the geographical distribution of the system, the evidence collected by an investigator may have different time zones. In order to prove that this evidence is legitimate in the court of law, Damshenas [12] suggested a specific time system for all the entities in the cloud. To overcome this issue, another researcher Mills [29] designed a network time protocol. This system will provide time synchronization between different computers. The current protocol is RFC 5905, It is the latest, and considered to be the most efficient protocol.

N. Complexity of Testimony

The court comprises people with little knowledge of computer especially of the complicated cloud commuting. Orton [30] suggested that a person well versed in cloud forensics should present the case so the court jury can comprehend the case in its true perspective. All the tasks completed during the investigation should be described in a simple way.

O. Documentation

Presenting your case in the court of law is the most important part. All the steps taken and all software and techniques used should be documented in order to prove the case. A slight mistake in the documentation will cost the case. Wolthusen [31] guided how a presentation should be written for forensics investigation.

P. Compliance Issues

In order to check which CSP is suitable for customer, Birk [13] suggested that the customers should check their compliance with the CSPs. CSPs should gain the trust of customers by providing them transparency, and that they can do this by involving a 3rd party investigator for conducting the investigation independently. Zawoad [8] stated providing preservation and proof of logs by CSPs will increase their auditability which is complusory if they're trying to form their cloud environment compliant with payment card industry.

Q. Blockchain Based Forensics Solution

Blockchain is a recent breakthrough in technology. The simplest explanation of blockchain is that it is an unchangeable database (Ledger) whoever owns it. It is based on Hash-function. Data once inserted in blockchain cannot be altered. The blockchain nodes broadcast the block on the basis of which a hash-code is generated for that block. This process is called proof of work. The first part of any forensics investigation is to reconstruct the incident to see what has happened. This is facilitated by t logs. All the problems related to t logs that we have covered in this paper do not nevertheless guarantee their 100% integrity. Logs can be altered in the cloud servers. Another main problem in cloud environment is the maintenance of the evidence storage and integrity of the evidence. Park [32] suggested a forensics framework which is blockchain based data storage and integrity management mechanism as blockchain ensures integrity of the data. Since all the blocks are connected to each other, integrity of the data can be simply verified by hash value of the preceding block. Another important part is to protect the logs [33]. Cloud makes a log for every activity that is carried out. A forensics investigator investigates the incident on the basis of logs. Because cloud is being simultaneously used by multiple users, who are sharing the same storage and processing network, maintaining confidentially of the users is the first priority of a forensics investigator. As discussed earlier in the transparency section, CSPs should be open to a third party investigator for checking integrity of logs. To overcome this issue, a log block tag system that is based on Merkle Hash Tree is available [34]. Pourvahab [35] purposed a cloud-based blockchain technology for IaaS model. In it, evidence is collected and stored in the forensic architecture of blockchain, in which peers are distributed among multiple nodes. A secure ring verification based authentication was purposed for protecting one’s device from unauthorized users.

XI. DISCUSSION

Different researchers have proposed a number of digital and cloud forensics models. Not all follow similar approaches. But the outcome of all of them are exactly the same. Ruan [16] was the first to introduce the term cloud forensics. This paper has been organized in the following sections. It provides methodologies for digital and cloud forensics, offering four steps for any digital or cloud forensics - identify, preserve, extract and present. Identification is the first stage where you have to collect all the evidence from the cloud environment which is the most difficult part of the process due to the geographical distribution of the system, usage of the same network by many users, and the processing speed. To prove that the incident has happened, cloud forensic investigators need to identify the type of incident (crime) and the assets which were used (data, software and hardware). In the identification stage, a warrant for search to access those CSPs infrastructure has to be issued. All the actions that took place to identify the valid evidence, and to notify methods and people used to investigate the crime, need to be properly recorded and documented. This should be done after identification, acquisition and collection of the evidence from the desired locations where they are stored in the cloud environment. The cloud forensics investigators need to separate digital evidences by disallowing unauthorized people to use the digital devices in which the incident occurred, or to even duplicate the digital evidence so that it cannot be used against the company. This involves well-trained personnel. The analysis stage involves extraction of the evidence from the identification and preserving stage, and then analysing the identified data. Well-trained personnel who are expert in their techniques are required to examine data and extract the evidence. The cloud forensics investigator probing the incident should have a high level of overview of the terrain. Otherwise, it will warrant delays. The cloud forensics investigators should review the stages encountered in the previous cases, and the training plans to find out different forensics techniques that can help him reduce the time of the examination. Presentation is the last stage in which the case is presented before the court of law. It is important to note that even a small mistake can lead to the dismissal of the case. That is why a well-documented report should be generated through those who are expert in evidence analysis. The report should be prepared in consultation with an expert who has command over the required legal procedure.Since the court normally has little knowledge of computers, it might be difficult for it to understand the cloud computing concepts. Therefore, the report should be presented in such a way that can help the court comprehend the facts and evidence.The report used and the supporting material such as the chain of evidence should be submitted in the court. Details about the crime such as the type of cloud incident, who is responsible, and other facts like compromised accounts, should be included in the report and submitted in the court.

XII. CONCLUSION

The cloud environment provides a lot of benefits to the users. Criminals also tend to take advantage of the system due to its complex structure. In this paper, cloud forensics problems have been identified and their solutions have been proposed to overcome the aforementioned security issues. Additionally, popular frameworks in digital forensics have been overviewed through a systematic literature review. First, this paper discussed all methodologies related to digital forensics (cloud forensics is a branch of digital forensic). Second, it highlighted the existing challenges in cloud environments regarding forensics, quoting references of the researchers who identified these challenges. Subsequently, the paper has provided all the purposed and implemented solutions designed and implemented by different researchers on cloud forensics, while also mentioning their functionalities.

Forensics software play an important role in criminal investigations. It is the need of the hour to develop a trustworthy software for cloud forensics. At present, all software in use for cloud forensics also support other branches of forensics, such as mobile and computer forensics, which the investigators can access. Furthermore, it is not possible to conduct forensics investigation by using these software due to the distributed nature of cloud. Therefore, software should be developed to support forensics investigation in cloud. This research provides future research directions to software developers, urging them to focus on specific areas of cloud in order to develop software to carry out forensics investigation.

References

[1] L. Columbus, (2021), *32% Of IT Budgets Will Be Dedicated To The Cloud By 2021*. https://www.forbes.com/sites/louiscolumbus/2020/08/02/32-of-it-budgets-will-be-dedicated-to-the-cloud-by-2021/?sh=2ac247545fe3 (accessed Jul. 07, 2021)

[2] McAfee, (2021), *Economic Impact of Cybercrime Report*. https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html (accessed Jul. 07, 2021).

[3] M. Herman, M. Iorga, A. M. Salim, R. H. Jackson, M. R. Hurst, R. Leo, *et al.*, "NIST Cloud Computing Forensic Science Challenges," *National Institute of Standards and Technology*, pp. 10-70, 2020. https://doi.org/10.6028/NIST.IR.8006

[4] R. McKemmish, *What is forensic computing?*: Australian Institute of Criminology Canberra, 1999.

[5] J. Robert, (2021), "60 Percent of Small Companies Close Within 6 Months of Being Hacked." https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/ (accessed Jul. 07, 2021).

[6] J. C.-L. Goh, S. L. Pan, and M. Zuo, "Developing the agile IS development practices in large-scale IT projects: The trust-mediated organizational controls and IT project team capabilities perspectives," *Journal of the Association for Information Systems*, vol. 14, p. 1, 2013. https://doi.org/10.1016/j.infsof.2008.01.006

[7] V. S. Harichandran, F. Breitinger, I. Baggili, and A. Marrington, "A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later," *Computers & Security*, vol. 57, pp. 1-13, 2016. https://doi.org/10.1016/j.cose.2015.10.007

[8] S. Zawoad, A. K. Dutta, and R. Hasan, "SecLaaS: secure logging-as-a-service for cloud forensics," in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, 2013, pp. 219-230. https://doi.org/10.1145/2484313.2484342

[9] T. Sang, "A log based approach to make digital forensics easier on cloud computing," in *2013 Third International Conference on Intelligent System Design and Engineering Applications*, 2013, pp. 91-94. https://doi.org/10.1109/ISDEA.2012.29

[10] P. M. Trenwith and H. S. Venter, "Digital forensic readiness in the cloud," in *2013 Information Security for South Africa*, 2013, pp. 1-5. https://doi.org/0.1109/ISSA.2013.6641055

[11] A. Pătraşcu and V.-V. Patriciu, "Logging framework for cloud computing forensic environments," in *2014 10th International Conference on Communications (COMM)*, 2014, pp. 1-4. https://doi.org/10.1109/ICComm.2014.6866662

[12] M. Damshenas, A. Dehghantanha, R. Mahmoud, and S. bin Shamsuddin, "Forensics investigation challenges in cloud computing environments," in *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, 2012, pp. 190-194.

[13] D. Birk and C. Wegener, "Technical issues of forensic

investigations in cloud computing environments," in *2011 Sixth IEEE international workshop on systematic approaches to digital forensic engineering*, 2011, pp. 1-10.

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

[15] A. Haeberlen, "A case for the accountable cloud," *ACM SIGOPS Operating Systems Review*, vol. 44, pp. 52-57, 2010. https://dl.acm.org/doi/abs/10.1145/1773912.1773926

[16] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud Forensics," in *Advances in Digital Forensics VII*, Berlin, Heidelberg, 2011, pp. 35–46. doi: 10.1007/978-3-642-24212-0_3.

[17] "Cloud SLAs: present and future: ACM SIGOPS Operating Systems Review: Vol 46, No 2." https://dl.acm.org/doi/abs/10.1145/2331576.2331586 (accessed Jul. 07, 2021).

[18] A. H. Busalim, A. R. C. Hussin, and A. Ibrahim, "Service level agreement framework for e-commerce cloud end-user perspective," in *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, Nov. 2013, pp. 576–581. doi: 10.1109/ICRIIS.2013.6716773.

[19] R. Hegarty, M. Merabti, Q. Shi, and B. Askwith, "found in Distributed Service Orientated Computing."

[20] Y. Shi, K. Zhang, and Q. Li, "A New Data Integrity Verification Mechanism for SaaS," in *Web Information Systems and Mining*, Berlin, Heidelberg, 2010, pp. 236–243. doi: 10.1007/978-3-642-16515-3_30.

[21] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 12, pp. 1947–1960, Dec. 2013, doi: 10.1109/TIFS.2013.2286456.

[22] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective Data

Access Control for Multiauthority Cloud Storage Systems,” *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 11, pp. 1790–1801, Nov. 2013, doi: 10.1109/TIFS. 2013.2279531.

[23] “Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics: Security & Forensics Journal Article | IGI Global.” https://www.igi-global.com/article/calm-before-storm/68408 (accessed Jul. 07, 2021).

[24] G. Sibiya, H. S. Venter, and T. Fogwill, *Digital forensic framework for a cloud environment*. International Information Management Corporation (IIMC), 2012. Accessed: Jul. 07, 2021. [Online]. Available: https://researchspace.csir.co.za/dspace/handle/10204/5890

[25] A. Juels and B. S. Kaliski, “Pors: proofs of retrievability for large files,” in *Proceedings of the 14th ACM conference on Computer and communications security*, New York, NY, USA, Oct. 2007, pp. 584–597. doi: 10.1145/1315245.1315317.

[26] J. Dykstra and A. T. Sherman, “Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques,” *Digit. Investig.*, vol. 9, pp. S90–S98, Aug. 2012, doi: 10.1016/j.diin.2012.05.001.

[27] D.-Y. Kao, “Cybercrime investigation countermeasure using created-accessed-modified model in cloud computing environments,” *J. Supercomput.*, vol. 72, no. 1, pp. 141–160, Jan. 2016, doi: 10.1007/s11227-015-1516-7.

[28] Z. Wan, J. Liu, and R. H. Deng, “HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing,” *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 743–754, Apr. 2012, doi: 10.1109/ TIFS.2011.2172209.

[29] “hjp: doc: RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification.” https://www.hjp.at/doc/rfc/ rfc5905.html (accessed Jul. 07, 2021).

[30] "Legal Process and Requirements for Cloud Forensic Investigations: Security & Forensics Book Chapter | IGI Global." https://www.igi-global.com/chapter/legal-process-requirements-cloud-forensic/73963 (accessed Jul. 07, 2021).

[31] S. D. Wolthusen, "Overcast: Forensic Discovery in Cloud Environments," in *2009 Fifth International Conference on IT Security Incident Management and IT Forensics*, Sep. 2009, pp. 3–9. doi: 10.1109/IMF.2009.21.

[32] J. H. Park, J. Y. Park, and E. N. Huh, "Block Chain Based Data Logging and Integrity Management System for Cloud Forensics," in *Computer Science & Information Technology (CS & IT)*, Sep. 2017, pp. 149–159. doi: 10.5121/csit.2017.71112.

[33] "Public Auditing of Log Integrity for Cloud Storage Systems via Blockchain | SpringerLink." https://link.springer.com/chapter/10.1007/978-3-030-21373-2_29 (accessed Jul. 08, 2021).

[34] "Merkle tree," *Wikipedia*. Jul. 01, 2021. Accessed: Jul. 08, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Merkle_tree&oldid=1031389060

[35] M. Pourvahab and G. Ekbatanifard, "Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology," *IEEE Access*, vol. 7, pp. 153349–153364, 2019, doi: 10.1109/ACCESS.2019.2946978.