Digital Forensics in Cloud Computing Platofrms

Iram Manan, Kashif Munir, Mubarak Almutairi

1. Department of Information Technology, Khwaja Fareed University of Engineering and Information Technology, Rahim Yar Khan, Pakistan
2. Faculty of Computer Science and Information Technology, Khwaja Fareed University of Engineering and Information Technology, Rahim Yar Khan, Pakistan
3. College of Computer Science & Engineering, University of Hafr Albatin, Saudi Arabia

Abstract
Cloud computing is most growing and fastest technology in the internet world. It is constructive for the many internet users from the last few years in the history of computing. Cloud storage is the most famous application of cloud computing. This application is mainly used to provide storage services to individuals and companies. However, several security issues occur due to the high growth of cloud computing. Many crimes are happening in the cloud computing field then. To secure the system, combined with Digital forensics, which works as cloud forensics. Cloud forensic is a more secure and fast performance for internet cloud users. This paper discusses the creative suitable forensics tools and frameworks that help secure cloud forensic systems. These tools are compared according to demand and research by different old researchers. This paper also discusses forensic readiness factors and mapping with cloud service models. Compare the application services models on base of challenges and solutions of cloud forensics.

Keywords:
Cloud Forensic, Cloud Forensic Tools, Digital Forensic Tools, C loud Service Models.

1. Introduction

Cloud computing has been an attractive topic and a preffered solution in the internet world and organizations in the last few years. (Zargari & Benford, 2016)(Alqahtany, Clarke, Furnell, & Reich, 2015). Cloud computing plays a vital role in providing a high extensible IT infrastructure. It offers experience services that increase flexibility, scalability, outstanding reliability, speed, and ample storage capacity at a low cost. There is no need to pay extra for administration resources or purchase physical infrastructure (Raghavan, 2013)(Yankson & Davis, 2019). In currrent years, it has a new model of information technologies but views it as a rapidly expanding and most performative technology in the past time of computing. (Alenezi, Atlam & Wills, 2019)(Ruan, Carthy, Kechadi & Crosbie, 2011). It also helps to change the system for services to create, manage, across, or deliver (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009). However, this technology's development and rapid growth make communication easier between criminals. According to a technical report published by the national crime agency 2014 (Narayana Samy, Shanmugam, Maarop, Magalingam, Perumal, & Albakri, 2018), criminals get a lot of advantages from the growth of technology due to the increase in crime in digital devices and investigations to cover the issue and challenges to define forensic solutions (Khanafseh, Qatawneh, & Almobaideen, 2019). Digital forensics is studied at "after-after thought, " a newly developed technology. Cloud computing growth in the industry as expected the armed compound growth related to 30% to $270 billion by 2020 (Prasad, 2016).

The national institute of standards and technology (NIST) acknowledges severe cloud issues organized by a cloud forensic. This group published a working draft NIST cloud computing Forensics science challenge. NIST categorized the forensic challenges in cloud computing as cloud forensic (Yankson & Davis, 2019). Investigation processes of digital crime depend on evidence, identifying the resources with critical information as proof of the crime. These are legal information acceptable by the court, stored, and transmitted digitally (Hargreaves, 20102). Digital forensics is disclosing and reporting electronic data (Hargreaves & Patterson, 2012).

The investigation process is more straightforward for forensic experts dealing with hardware devices such as memory cards, flash drives, complicated instruments, etc. When any attack over cloud computing environment, this process makes a low report, so we use the forensic services to create a more severe and control the collection of data from consumers and evidence that incidentally over. Digital investigation facilitates saving money and time; some services could be based on the different services model, which are a software as a Service (SaaS), Platform as Services (PaaS), Infrastructure as Services (IaaS).

New technology has new security challenges and risks to protect user data. Cloud forensics also helps protect and provide security on data security challenges, including user authorization, the privacy of data, and access control. For cloud-based forensic evidence using given treat and retrieve the data is timely manners in the operating system, host of hardware hypervisor, host OS, web services of amazon, and network elements. The cloud forensic challenges and provide existing solutions based on the

Manuscript received April 5, 2022
Manuscript revised April 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.4.72

result of analysis of paper identification. The current solutions overcome the cloud forensic importance in the organization's readiness (Alenezi, Atlam & Wills, 2019) and cover the categorization of challenges based on technically legal and organizational.

Digital forensics: Digital forensics is an independent field developed in SaaS when the popularity of computer crime increased due to internet surgery. It analyses electronic information stored in digital or virtual machines to regenerate and regulate the sequence of specific incidents. It go well with ordinary because of the growth of technology and powerfull dependence on technology. From 20th century, it has been scientifically based on the idea of methods and techniques acceptable in the court.

The organization's main aim is to increase its profit margin with cost control. They want to increase profit margin by using new services and technologies. Cloud helps decrease costs and gives advanced and automated infrastructure and maintenance with high security and productivity. Every business company has its shadow, and the CSP provides these services to the companies after signing the contract with them. A CSP has the responsibility to maintain the infrastructure used for the benefits of the cloud to customers via the cloud internet. All services and maintenance of cloud computing are controlled remotely. The Services Model of the cloud also gives some cloud characteristics that we mentioned above, services models of cloud used, and the cloud deployment models.

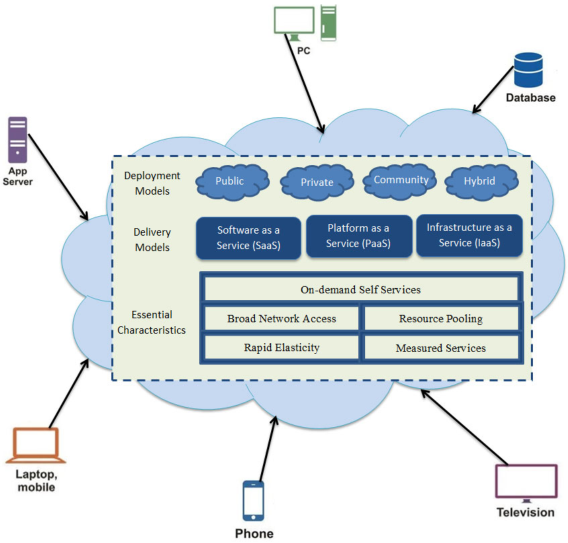

Figure 1: Cloud Computing

According to the traditional environment's comparison with the cloud, the cloud service gives a lot more advantages to the customers. The conventional solution provides limited access, storage, and scalability worldwide. Now the investment is not the crucial concern for the maintenance and infrastructure.

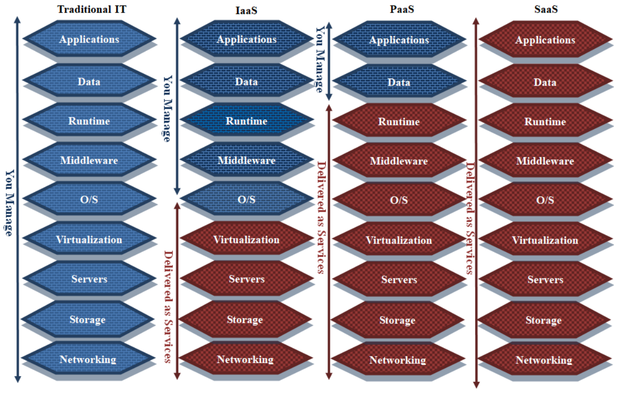

Figure 2: Cloud Computing and Traditional IT comparison

Nowadays, everyone interacts with the internet in the digital technology world due to rapidly increasing online crimes. See in Figure:

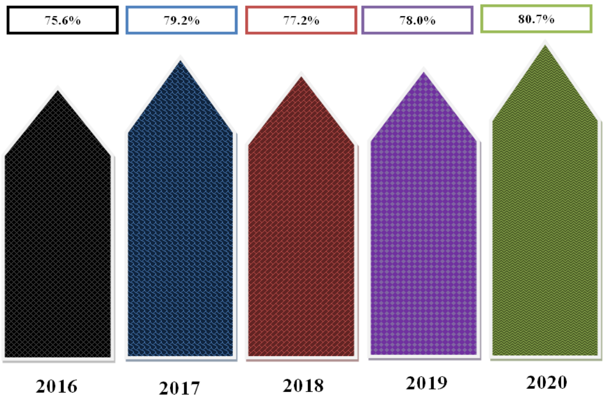

Figure 3: Cyber Security attacks of the last five-year percentage

This system immediately affects people who won't use digital evidence for the help of law enforcement to expose digital crimes. Investigators use the digital forensic process to search for correct digital proof in digital forensics. Different digital forensic tools and techniques are developed to help the investigator in the investigation process, which aims to recognize, maintain, gather and inspect evidence. In digital forensics, it is a vital component of the chain of custody and integrity maintenance in digital proof. Some types of changes or damage in the digital evidence make them unacceptable in court.

Cloud forensics is a subsection of digital forensics, and this needs the digital investigation process according to digital principles and procedures in the cloud environment. Different issues are compared to the digital and network investigation in the cloud environment. According to NIST, cloud forensics is the scientific principles application, technological practices, and acquired ways to reconstruct the past cloud computing events through identification, preservation, collection, Examination, reporting, and presentation of digital evidence.

2. Cloud service models

Figure 4: Three Cloud Services Models

2.1 Infrastructure-as-a-Service (IaaS)

The IaaS service model that CSPs give a hardware infrastructure/V.M., networking devices, etc., also provides device security and housing. The customer will be capable according to the need. The customer has predominantly control period circumventing purchasing, housing, and controlling basic hardware and software infrastructure.

2.2 Platform-as-a-Service (PaaS)

PaaS is a software deployment service model. The CSP provides a platform to the customer for uploading and maintaining their system and applications without any tension about the infrastructure maintenance and system work. It does not permit full access because it may make it difficult for the investigators.

2.3 Software-as-a-Service (SaaS)

The SaaS is a delivery and software licensing model used for subscription licensing and centrally hosted. It also helps reduce costs because it doesn't wholly control software and hardware development. Nevertheless, it provides less power and can make it very complex for the investigator.

3. Cloud Forensics Tools

(Škrinárová & Vesel, 2016)This work concentrates on the issue of a superior computing education given frameworks, for example, lattice, cloud, (Sriharsha, 2012) They have presented a combined study of different models. They work over the models of the education system. This work is enhanced work for learning strategies. After this, they have again presented an enhanced study.

3.1 FROST

FROST is an open stack forensics tool that is used in the platform of cloud computing platforms. This tool is used to get the data for digital forensic investigation from virtual disks, API logs, and guest firewall logs. It provides Infrastructure-as-a-Service (IaaS) cloud. It restores the data in the form of cryptography after accumulating log data in Hash trees. The virtual machines do not need to interconnect with the operating system and work at the cloud management plane. The FROST tools are user-friendly, so the customer and forensics investigators do not have any connection with the cloud service provider for law enforcement.

3.2 OWADE

Offline Windows Analysis and Data Extraction (OWADE) is open-source software. It is used to find out the user visited a website to check if there is any data stored in the cloud by encryption bypass on the hard drive of a personal computer.

Commercial forensic software retrieves files from a di sc, which isn't very helpful in comprehending online behav ior. The bulk of sensitive data on a hard disc, such as browser history, site logins, and passwords, is encrypted using an algorithm based on the basic Windows login.

3.3 CloudTrail

CloudTrail is the service of AWS that gives permission to manage AWS account operations, risk management compliance, and governance. Events are created in CloudTrail when a user, role, or AWS service acts. AWS Events include console management, APIs, Command Line Interface, and SDKs.

AWS CloudTrail provides audits, security monitoring, and operational troubleshooting by recording user behavior and API usage. CloudTrail logs, continually monitor, and maintain account activity connected to AWS infrastructure tasks, providing you control over storage, analysis, and corrective actions.

3.4 Cloud Data Imager

Cloud Data Imager is a library (CDI Lib). It is a mediation layer that provides reading access to metadata and files in specified remote folders while delivering a consistent front end that hides the syntactic and functional differences across cloud platforms. It presently offers access to some storage services. On top of the library, a demo application has been constructed that allows directory navigation, file content viewing, and imaging of folder trees with export to standard forensic formats. The Cloud Data Imager project seeks to fill the void left by Quick and Choo's work.

3.5 DFF

The Digital Forensics Framework is an open-source platform. All over the world, mainly educational institutes, private companies, and law enforcement agencies use this tool. It can do the cryptographic hash computation, scripting, EXIF meta-data extraction, automatic reporting of vital information web browser, import all Microsoft Outlook mailboxes, memory dump analysis, batching capabilities, and data may be extracted automatically.

3.6 ForenVisor

ForenVisor is a lightweight hypervisor explicitly designed for dependable live forensics. It is used to increase live data and storage dependability by focusing on three areas. It reduces code size and prevents the forensic process from being interfered. It gathered the entire system state, data process, raw memory, and input/output data directly from the hardware without turning on device drivers. Finally, it saves volatile data to disc and safeguards it with the File safe module. The File safe module can also provide security for sensitive files, such as forensic logs, in the guest O.S.

3.7 Encase eDiscovery suite

EnCase eDiscovery is a powerful tool for various issues, including government and internal investigations. It can instantly seek and collect data from a broad scope of sources without jeopardizing the data's integrity.

The development of distributed and remote workforces, the proliferation of mobile devices, and novel data sources are all addressed by eDiscovery gathering technologies. Defensibility requires comprehensive data collection across all data sources, including endpoints such as PCs and laptops. Collection analytics and culling are critical to conducting effective digital investigations since they restrict the document collection to reduce the expense of legal review.

3.8 X-Ways

X-Ways is a market-available exclusive origin. It is a computer forensic software package that includes WinHex and Disk Imager. It provides full access to drives, RAIDs, and pictures with a size larger than 2 GB, the carving of documents, identifying recognized images using PhotoDNA hashing. Multiple hashing values may be produced simultaneously.

3.9 Wireshark

Wireshark is the most widely used network protocol analyzer in the world. It allows viewing what incidents occur in-network at a microscale level. It is the de facto for numerous businesses, charitable organizations, Govt. branches, and educational institutions. Wireshark development flourishes due to the volunteer contributions of networking specialists worldwide, and it is the continuance of a project.

3.10 Wildpackets Omnipeek40

Omnipeek is a high-performance network protocol analyzer that can decode hundreds of protocols for quick network troubleshooting and diagnostics everywhere network problems occur. Omnipeek Network Analyzer delivers real-time network monitoring and analysis.

3.11 Network Miner

Network Miner is a Network Forensic Analysis Tool (NFAT) for Windows. It is used to detect operating systems, open ports, sessions, etc., as a packet of passive network capturing tools.

It simplifies complex Network Traffic Analysis (NTA) by displaying retrieved artifacts in an easy-to-use user interface. It presented data simplifies analysis and saves the analyst or forensic investigator considerable time. It is a well-liked tool among incident response teams and law enforcement. Today, it is utilized by businesses and organizations worldwide.

Table 1: Analysis of Wireshark, Omnipeek, Network-Miner Forensic tools on Cloud Enviornment

	Wireshark	Omnipeek	Network-Miner
Parsing of network streams	×	×	×
DNS traffic analysis	×	×	×
HTTP-header data extraction	×	×	×
SSL Data extract	×	×	-
Communication partner List	×	×	-
Cloud Based communication storage	-	-	-
Current traffic Cloud	-	-	-

Based	🟥	🟩	🟪

3.12 Kumodd

Kumodd is an accession tool for cloud drives. It is used as the service provider's API to fully acquire the data of a cloud drive and store it in a suitably formatted local filesystem tree. It is divided into three logical layers: drivers, dispatcher, and user interface. It helps four critical services and solves two client-based acquisition issues we identified: limited data duplication on the client and recapture the alteration. The accession of cloud-native artefacts without an explicit file representation, such as Google Docs, takes snapshots in standard formats such as PDF.

3.13 Kumofs

Kumofs' primary goal is to bridge the denotative space within cloud artefacts and older file-based technologies. It is performed next to exposing in the cloud drive about file system interface, i.e., implementing a FUSE file system to mount the disc remotely. It enables it to be explored, triaged, and selectively acquired using standard command-line tools such as ls and cp.

Kumofs comprises five functional modules: the filesystem, authentication, command line, query processor, and cache manager. Kumofs, by default, offers entries in virtual files for the various export formats.

3.14 Kumodocs

Kumodocs was created expressly for use with Google Docs, which uses the way online programs store and operate with such artifacts. It aids in the reverse engineering of the internal changelog data structure, which records the whole modification document history to the position that it can be stored and interpreted independently to a helpful stage.

3.15 LINEA

Live Network Evidence Acquisition (LINEA) is a technique for collecting LINE to develop and test a full-fledged prototype. It has been demonstrated to be forensically sound, which means that the obtained evidence is resilient and can be confirmed at any moment after acquisition. The correlation of information from many ways of evidence improves robustness characteristic, while encryption, time stamp, and digital sign the acquisition output improve the dependability.

LINEA launches a new Collector VM instance for the investigator to ensure integrity and security each time a new acquisition session is established. If the Collector VM becomes damaged or hacked during an acquisition session, preventing the issue from spreading. Using a dedicated VM also provides dependability, robustness, and scalability benefits.

3.16 Encase remote agent

The EnCase agent works in the background on system endpoints such as desktop computers and does not communicate with its users. This product enables applications from the vendor's complete product line to operate on system endpoints.

Encase has long been used to retrieve evidence from appropriate hard drives. Encase investigator collects evidence such as papers, photos, internet history, and Windows Registry information from the user file investigation process. EnCase training and certification are also available through the firm.

3.17 Snort

SNORT is a network intrusion detection system built in the C computer language. It is open-source software that is available for free. It may also be used as a real-time packet sniffer to monitor the system. The network administrator identifies the dangerous packet to the design and monitors incoming packets using the snort. It is based on a packet capture tool from a library. The rules may be implemented in any network environment or operating system that is easy to build and appeal to. It monitors real-time traffic, content matching, protocol analysis, OS fingerprinting, generate logs, and performs packet recording.

3.18 EnCase Forensic

EnCase is a guide. The software has risen to become a computer forensic software and services the market leader. Its solutions help enterprises, governments, and law enforcement agencies to conduct successful digital investigations, respond quickly to eDiscovery requests and other large-scale data collecting requirements, and respond decisively to external threats.

It can investigate/analyze several machines simultaneously in a secure manner. With quick reaction capabilities, you can reduce the effect of an incident and avoid system downtime. Researches and analyses a variety of platforms. Collect only possibly relevant data in an efficient manner. Examine huge groups of devices for sensitive or classified data. Detect fraud, security incidents, and difficulties with staff integrity.

3.19 Sleuthkit

Sleuthkit is a group of command-line file and volume system forensic investigation tools for UNIX-based operating systems. Analyzes raw, Expert Witness (including Encase), and AFF file system and disc images. Various analysis techniques-meta-data structure analysis, timeline construction, non-intrusive Examination of file systems, allowing deleted and hidden content. The Sleuth Kit provides over 21 powerful Linux-based tools organized into nine unique categories.

3.20 AccessData Forensic Toolkit (FTK)

AccessData Forensic Toolkit (FTK) has supplied investigators with digital forensic tools that work together to read, acquire, decrypt, analyze, and report on digital evidence. It allows law enforcement and business security specialists to conduct comprehensive computer forensic examinations. It is used for cultivated code-breaking and password recovery, and it supports complete Unicode and code page support. It also has advanced email support, a powerful search engine, and registry supplemental reports. It's simple to use as an interface.

3.21 FTK Imager

FTK Imager is an open-source program developed by Access Data used to generate exact duplicates of objective evidence without any update. The image of the actual evidence stays un-updated, allowing us to duplicate data at a considerably quicker rate, which can then quickly keep an estimate further. It additionally has an integrity testing function that creates a hash report that aids in comparing the hash of the evidence before and after making the image of the actual evidence. A forensic picture can also be backed up or tested without affecting the real copy or proof.

3.22 Autopsy

An autopsy is a graphical user interface for Sleuthkit. Autopsies are utilized for both dead and live analysis. It includes case management, numerous analysis techniques such as meta-data structure analysis, keyword search, picture integrity timeline production, and the ability to organize files according to their kind, among other things. Because it is open-source, it inherits the security concepts that all open-source projects benefit from, such as the ability for anybody to review the code and detect any harmful intent on the authors.

3.23 FIT4D

Forensic Investigation Toolkit 4 Developing Nations is a software toolkit that uses developing countries' limited resources. It increases efficiency, privacy, and usefulness while addressing the shortage of forensic professionals in underdeveloped nations. The FIT4D software toolkit will be deployed via a low-cost, distributed infrastructure.

3.24 UFED CLOUD ANALYZER BASICS

Cloud Analyzer is a Windows-based extraction and analysis program that allows you to import a file containing account login from major cloud providers. This extraction may be performed using a UFED physical analyzer utilizing either a file system or physical extraction of the memory of a smartphone. The investigators can input usernames and passwords manually. The UFED Cloud Analyzer then uses the service provider's application programming interface (API) to capture "snapshots" of private cloud-based evidence.

3.25 WinHex

WinHex is a sophisticated data analysis, editing, and recovery application. It is a worldwide hexadecimal editor that may be used in computer forensics, low-level data processing, data recovery, and information security. It examines and modifies various document types and recovers digital devices' lost or removed data. It has built-in support for RAID systems and dynamic storage. Its functions as a RAM editor, disc editor, and data interpreter.

3.26 Active File Recovery

It is a data recovery program that aids in the recovery of files from formatted hard drives or partitions. Also, it restores data from the Windows Recycle Bin after it has been emptied. The program supports all digital devices supported by Windows, Macintosh, and Linux. Because of the 64-bit executable version, the newest edition provides much quicker scan times. Because it has more processing power and memory, it scans faster. In addition to the handful of file signatures supported by the previous version, version 12 of active file recovery now enables file signatures for files of uncommon kinds. Files can also be ordered depending on several properties.

3.27 ProDiscover

ProDiscover is a used tool for examining the security of hard discs. It includes a reporting tool for presenting findings as evidence in legal proceedings and aids in collecting time zone data, driving statistics, and Internet activities. It offers powerful search features to capture unique data, document names and documents kinds, data patterns, date ranges, etc. It supports data content and cluster views.

Table 1: Analysis of WinHex, Active File Recovery, ProDiscover Basic Forensic tools on Cloud Enviornment

Parameters	WinHex	Active File Recovery	ProDiscover Basic
Help Disk Images	Raw DD.	Raw DD, DIM	Raw DD, eve
File Analysis	√	√	√
Log Analysis	√	√	√
Index Deleted File	×	√	√
Index Files	√	√	√
Analysis of Memory Dump	√	√	√

4. Cloud Forensics Tools Categorization

Table 3: Cloud Forensic tools Categorization

Utilized Tools	General/ Cloud Established
FROST	Cloud Established
OWADE	Cloud Established
CloudTrail	Cloud Established
Cloud Data Imager	Cloud Established
VNsnap	Cloud Established
Kumodd	Cloud Established
Kumofs	Cloud Established
Kumodocs	Cloud Established
LINEA	Cloud Established
ForenVisor	Cloud Established
Encase e-discovery suite	General
X-Ways	General
X-Ways Forensic	General
Wildpackets Omnipeek40	General
Encase remote agent	General
Network Miner	General
Snort	General
EnCase Forensic	General
Wireshark	General
Sleuthkit	General
AccessData Forensic Toolkit (FTK)	General
FTK Imager	General

5. Cloud Forensics Tools Mapping with Service Models

This study is based on the student of NCBA&E Bahawalpur Campus. As we know, human behavior differs from area to area and intellectuality. Modern countries are spending their central part of the budget on the practical education of the students. Our primary focus is on the students' learning ability in this study.

Table 4: Cloud Forensic tools mapping with Cloud Services Models

Tools	Applicable to Services Model		
	IaaS	PaaS	SaaS
DFF	√	×	×
EnCase Forensic	√	×	×
AccessData Forensic Toolkit (FTK)	√	×	×
Wireshark	√	×	×
Wildpackets Omnipeek40	√	√	√
NetworkMiner	√	√	√
X-Ways Forensic	×	×	√
FROST	√	×	×
Kumodd	×	×	√
Kumodocs	×	×	√
Kumofs	×	×	√
VNsnap	√	×	×
Cloud Data Imager	×	×	√
LINEA	×	×	√
ForenVisor	√	×	×

6. Cloud forensic frameworks

Many frameworks are designed for different branches of digital forensics, and other frameworks cover different departments, especially or according to the need. All frameworks have various types of features according to the proposed strategy. Frameworks are used to collect evidence for the investigation process and with many stages covering the investigation process for implementation.

Table 5: Cloud Forensic Frameworks mapping with Cloud Forensic Stages

Frameworks	Stages					
	Identification	Preservation	Collection	Examination and Analysis	Reporting and Presentation	Other
Hogan	√	√	√	√	×	×
NIST	×	×	√	√	√	√
Open Cloud	√	√	√	×	×	√
Ruan	√	√	√	√	×	√
Shah	√	√	√	√	×	×

IDFPM	×	√	√	√	√	√
DIP					×	
Martini	√	√	√	√	×	×
Shah	√	√	√	√	×	×
Fundamental overarching	√	×	×	√	√	×
McKemmish	√	√	×	×	√	√
Adams Process	√	×	×	×	×	√
Analysis Cycle					×	
SLA for FaS	√	√	√	√	×	×
RSA	√	×	×	√	√	×
FAAS	√	√	√	×	√	×
Manual	√	√	√	√	×	×
Bhatia	√	×	×	×	×	×
Khanafseh	√	×	×	×	×	×
iCFR	×	√	√	√	√	×
Vadlamudi	√	√	√	√	×	×
Event-Based	×	×	×	×	√	×
Alqahtany	√	√	√	√	√	×
Farina	×	×	×	×	√	×

7. Cloud forensic readiness factors

7.1 Technical Factors

The technological components indicate the component that can affect forensic preparedness in the cloud. These are related to digital forensic preparedness, which is discussed further down.

Cloud infrastructure

Cloud infrastructure prepares infrastructure fundamentals to support digital forensic investigations. It could be helpful for the organizations to properly determine, detect, and preserve possible pieces of evidence. It includes the server, storage, operating system, networks, and digital forensic libraries.

Cloud architecture

It is necessary to design in a way that can expand the forensic capacity. The faultless architectonics that helps cloud forensics will smooth forensic processes and give results to get acceptable digital pieces of evidence.

Forensic technologies

Forensic technologies such as trained tools, software, and hardware may help the organization control all forensic investigations. Those played an essential role in collecting digital evidence in cloud environments. It may be hard to perform digital studies without existing technologies, and the results of these technologies should be accurate and reliable to provide acceptable results.

Cloud security

Cloud computing security can play an essential role in digital forensic work as the activated alarm helps generate the notifications when matching the specified criteria. It also provides a secure environment that is helpful to find the process of digital evidence and the origin of evidence. Therefore, to perform the digital investigation, first, it must detect the incidents by a monitor system on time. It is possible by using different technologies such as intrusion detection systems (IDSs), Anti-virus, and Anti-spyware technology. Furthermore, the collected evidence must be securely gathered, stored, and transported in a secure location.

7.2 Organizational Factors

Management support

Support management factor requires top organizational management, which is helpful for the organization to accomplish the forensic readiness and authentication, decision-making, funding, and required resources. The corporate peak level management must know the importance of forensic readiness and its establishment impact on digital investigation and implementation of the enthusiasm.

Readiness Strategy

A readiness strategy is an organizational scheme to accomplish forensic readiness. Commonly, this scheme is concerned with the enthusiasm of how it would work. Achieve forensic readiness, and organizations should be form committed strategic objectives that serve the organization's needs. Its strategy should be flexible to adjust to the potential changes. The organization's readiness strategy includes budget planning, hypothetical scenarios, and possible evidence sources.

Governance

Governance covers the implementation management of cloud forensic processes and composition, identifying authorities, and operations. This factor includes the organization's general policy on cloud forensic readiness, such as managing forensics operations, collecting digital evidence, and accomplishing successful investigations. Verify that all procedures and controls are structured accurately to conduct a successful forensic analysis.

Besides, governance can verify the quality of forensic readiness in an organization.

Culture

Culture is a pattern of values, beliefs, assumptions, and practices that directly impact forensic readiness. Before forensic readiness is compulsory to understand or change the culture, it is helpful for a successful forensic investigation.

Training

The training factor is related to providing training programs to technical staff and conducting awareness programs for non-technical staff for forensic best practices. For successful forensic readiness, the organization needs to run training programs that certify their technical team and up-to-date knowledge and skills related to forensics. These training and awareness programs provide knowledge that helps to minimize the chances of loss of evidence.

Procedures

Procedures include the organization's general privacy and safety policies through digital investigations. Organizations need to clear all-forensic policies and also which possible to collect admissible evidence. This factor includes the principles, methods, and directions that help design digital forensics investigations. It also covers reactive and proactive forensic schemes.

7.3 Legal Factors

Service Level Agreements (SLA)

SLA is a contract signed by the CSP and customer that have stated the offered with forensic investigation. SLA has all details clearly about the responsibilities of CSP and customers, which are associated with forensic analysis.

Regulatory

Regulatory factors concerned the constancy of laws and regulations, such as the chain of custody and acceptance of evidence in the court. To accomplish forensic readiness, organizations must have the knowledge and awareness to adapt to appropriate rules, regulations, laws, and policies. Additionally, cloud providers must attach to the restrictions imposed on service providers

Jurisdiction

Jurisdiction is the judicial region; CSP has access to one or more areas where it provides the cloud from the different regions or areas. The organization must determine the judicial parts; it would be considered if CSP offers services in one or multi-jurisdiction. The services agreements have not mentioned that multi-jurisdiction and data do not exist in related jurisdictions during the investigation process, which can cause critical problems for the organization. Moreover, organizations should have a more precise knowledge of applicable jurisdictions' requirements.

Table 6: Cloud Forensics Readiness Factors Mapping to the Literature

Technical Factors				Organizational Factors						Legal Factors		
Infrastructure	Architecture	Technologies	Security	Management support	Strategy	Governance	Culture	Training	Procedures	SLA	Regulatory	Jurisdiction
×	√	×	√	×	×	×	×	×	√	√	√	√
√	×	√	×	×	×	√	√	√	√		√	√
×	×	√	×	×	√	×	×	×	√	√	×	√
√	√	√	×	√	×	√	√	√	×	×	√	×
×	√	√	√	×	×	×	×	×	×	×	×	√
√	×	√	√	×	×	×	×	×	×	×	×	×
×	×	√	√	×	√	√	×	√	√	×	√	√
√	×	√	√	×	√	×	×	×	×	×	√	√
×	√	√	×	√	×	√	√	√	×	×	√	×
×	√	×	√	×	×	×	×	×	√	×	×	√
×	×	×	√	×	×	×	×	×	√	√	√	√
×	×	×	×	×	×	×	×	√	√		×	×
×	×	√	×	×	×	×	×	×	√	√	×	√

Table 7: Forensic Artifacts in All Forensic Contributors/Stakeholders with Dependency

Contributors /Stakeholder	Resources and Access mechanisms	Forensics Artifacts	Dependency		
			CSP	CEU	CSO

s					
Cloud end-user	APIs	Data revision, Directory listing, changelog, and metadata information	√	×	×
	Mobile	Database and Log files	×	√	×
	Desktop application	Database files, Application logs, registry, network captures, and event logs/Syslog	×	√	×
	Browser	Browser cache, history, and cookies	×	√	×
Cloud service owner	APIs	Account service, activities, data logs, and application	√	×	√
	CLI	Account service, activities, data logs, and application	√	×	√
	Console Management/dashboard	Account service, activities, data logs, and application	√	×	√
Virtual machine	APIs	Firewall, Guest OS, anti-malware/ antivirus, VM snapshots and clones, IDS/IPS logs, database and application backups, application log files, flow logs/network, transaction logs	√	×	√
	CLI	Firewall, Guest OS, anti-malware/ antivirus, VM snapshots and clones, IDS/IPS logs, database and application backups, application log files, flow logs/network, transaction logs	√	×	√
	Console Management/dashboard	Firewall, Guest OS, anti-malware/ antivirus, VM snapshots and clones, IDS/IPS logs, database and application backups, application log files, flow logs/network, transaction logs	√	×	√
CSP (Hypervisor)	APIs	Syslog/Events based logs, messages and audit based logs, proc folder and /var /log	√	×	×
	CLI	Syslog/Event-based logs, messages and audit based logs, proc folder and /var /log	√	×	×
	Console Management/dashboard	Syslog/Event-based logs, messages and audit based logs, proc folder and /var /log	√	×	×
CSP (Cloud management software)	APIs	Different logs connected with various elements of the cloud environment such as VMs, cloud network, cloud storage, hypervisor	√	×	×
	CLI	Different logs connected with various elements of the cloud environment such as VMs, cloud storage, hypervisor	√	×	×
	Console Management/dashboard	Different logs connected with various elements of the cloud environment such as VMs, cloud network, cloud storage, cloud network, hypervisor	√	×	×
CSP (Cloud storage management)	APIs	Snapshots, Backups, replicas, logs, and archives databases	√	√	√
	CLI	Snapshots, Backups, replicas, logs, and archives databases	√	√	√
	Console Management/dashboard	Snapshots, Backups, replicas, logs, and archives databases	√	√	√
CSP (Cloud network management)	APIs	Gateway logs, switches, Router, SDN controller, southbound logs of APIs, northbound	√	√	√
	CLI	Gateway logs, switches, Router, SDN controller, southbound logs of APIs, northbound	√	√	√
	Console Management/dashboard	Gateway logs, switches, Router, SDN controller, southbound logs of APIs, northbound	√	√	√

8. Conclusion

In the cloud environment, the service providers and customers must work together. Cloud computing has come in cloud forensics when some security incidents occur in the cloud environment. Some of the challenges are proposed by some researchers, and some potential solutions are also offered based on challenges. But still, some open issues have not been solved that need to tackle. Some researchers suggest some forensic tools to solve some problems, and some frameworks are also recommended. Many of the challenges are solutions that depend on the CSP officer related to delay response, trust issues, or trust issues by the customer or CSP officer and evidence acquisition. Problems occur in the investigation process with evidence form, how tackle challenges and apply the solutions, researchers work on remaining issues future attacks.

References

[1] Dykstra, J., & Sherman, A. T. (2013). Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. Digital Investigation, 10, S87–S95. https://doi.org/10.1016/j.diin.2013.06.010

[2] Bursztein, E., Fontarensky, I., Martin, M., & Picod, J.-M. (2011). Beyond files recovery OWADE cloud-based forensic. BlackHat.

[3] Amazon Web Services, "AWS CloudTrail : User Guide," 2016.

[4] Federici, C. (2014). Cloud Data Imager: A unified answer to remote acquisition of cloud storage areas. Digital Investigation, 11(1), 30–42. https://doi.org/10.1016/j.diin.2014.02.002

[5] Almulla, S., Iraqi, Y., & Jones, A. (2016). Digital forensic of a cloud based snapshot. 2016 Sixth International Conference on Innovative Computing Technology (INTECH).

[6] Roussev, V., Ahmed, I., Barreto, A., McCulley, S., & Shanmughan, V. (2016). Cloud forensics–Tool development studies & future outlook. Digital Investigation, 18, 79–95. https://doi.org/10.1016/j.diin.2016.05.001

[7] Roussev, V., & McCulley, S. (2016). Forensic analysis of cloud-native artifacts. Digital Investigation, 16, S104–S113. https://doi.org/10.1016/j.diin.2016.01.013

[8] Castiglione, A., Cattaneo, G., De Maio, G., De Santis, A., & Roscigno, G. (2019). A novel methodology to acquire live big data evidence from the cloud. IEEE Transactions on Big Data, 5(4), 425–438. https://doi.org/10.1109/tbdata.2017.2683521

[9] Qi, Z., Xiang, C., Ma, R., Li, J., Guan, H., & Wei, D. S. L. (2017). ForenVisor: A tool for acquiring and preserving reliable data in cloud live forensics. IEEE Transactions on Cloud Computing, 5(3), 443–456. https://doi.org/10.1109/tcc.2016.2535295

[10] Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. Computer Law and Security Report, 26(3), 304–308. https://doi.org/10.1016/j.clsr.2010.03.002

[11] OpenText Security. (n.d.). EnCase information assurance. OpenText. Retrieved March 26, 2022, from https://security.opentext.com/encase-information-assurance?utm_source=ediscovery&utm_medium=redirect.

[12] Software for computer forensics, data recovery, and IT security. (n.d.). X-Ways.Net. Retrieved March 26, 2022, from https://www.x-ways.net/.

[13] Quick, D., & Choo, K.-K. R. (2013). Dropbox analysis: Data remnants on user machines. Digital Investigation, 10(1), 3–18. https://doi.org/10.1016/j.diin.2013.02.003

[14] Spiekermann, D., Eggendorfer, T., & Keller, J. (2015). Using network data to improve digital investigation in cloud computing environments. 2015 International Conference on High Performance Computing & Simulation (HPCS).

[15] Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Digital Investigation, 9, S90–S98. https://doi.org/10.1016/j.diin.2012.05.001

[16] (N.d.). Opentext.Com. Retrieved March 26, 2022, from https://security.opentext.com/encase-endpoint-investigator.

[17] Zafarullah, Anwar, F., & Anwar, Z. (2011). Digital Forensics for Eucalyptus. 2011 Frontiers of Information Technology.

[18] (N.d.-b). Snort.Org. Retrieved March 26, 2022, from https://www.snort.org/.

[19] Wireshark · Go Deep. (n.d.). Wireshark.Org. Retrieved March 26, 2022, from https://www.wireshark.org/.

[20] (N.d.-c). Sleuthkit.Org. Retrieved March 26, 2022, from http://www.sleuthkit.org/index.php.

[21] Ruan, K., James, J., Carthy, J., & Kechadi, T. (2012). Key terms for service level agreements to support cloud forensics. In IFIP Advances in Information and Communication Technology (pp. 201–212). Springer Berlin Heidelberg.

[22] AccessData Group, Inc. (2019, February 25). Products and services. AccessData. http://accessdata.com/products-services/.

[23] Dykstra, J., & Sherman, A. T. (2011). Understanding Issues In Cloud Forensics: Two Hypothetical Case Studies. 1–10.

[24] Shah, J. J., & Malik, L. G. (2013). Cloud Forensics: Issues and Challenges. 2013 6th International Conference on Emerging Trends in Engineering and Technology.

[25] Poston, H. (n.d.). 7 best computer forensics tools [updated 2021]. Infosec Resources. Retrieved March 26, 2022, from https://resources.infosecinstitute.com/topic/7-best-computer-forensics-tools/

[26] Sanap, V., & Mane, V. (2016). Comparative study and simulation of digital forensic tools. https://www.semanticscholar.org/paper/fe8d5a54d09f3ef2569e3f6079af794e3dd9c02b

[27] Naaz, S., & Ahmad, F. (2016). Comparitive study of cloud forensics tools. Communications on Applied Electronics, 5(3), 24–30. https://doi.org/10.5120/cae2016652258

[28] Manson, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M., & Treichelt, J. (2007). Is the open way a better way? Digital forensics using open source tools. 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07).

[29] Kamble, D. R., & Jain, N. (n.d.). Digital forensic tools: A comparative approach. Embeddedsw.Net. Retrieved March 26, 2022, from https://embeddedsw.net/doc/Openpuff_paper_Digital_forensic_tools_a_comparative_approach.pdf

[30] Zargari, S., & Benford, D. (2012). Cloud Forensics: Concepts, Issues, and Challenges. 2012 Third International

Conference on Emerging Intelligent Data and Web Technologies.

[31] Alqahtany, S., Clarke, N., Furnell, S., & Reich, C. (2015). Cloud forensics: A review of challenges, solutions and open problems. 2015 International Conference on Cloud Computing (ICCC).

[32] Raghavan, S. (2013). Digital forensic research: current state of the art. CSI Transactions on ICT, 1(1), 91–114. https://doi.org/10.1007/s40012-012-0008-7

[33] Yankson, B., & Davis, A. (2019). Analysis of the current state of cloud forensics: The evolving nature of digital forensics. 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA).

[34] Alenezi, A., Atlam, H. F., & Wills, G. B. (2019). Experts reviews of a cloud forensic readiness framework for organisations. J. Cloud Comput. Adv. Syst. Appl, 8(1).

[35] Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud forensics: An overview. Advances in Digital Forensics, 7, 35–49.

[36] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generations Computer Systems: FGCS, 25(6), 599–616. https://doi.org/10.1016/j.future.2008.12.001

[37] Narayana Samy, G., Shanmugam, B., Maarop, N., Magalingam, P., Perumal, S., & Albakri, S. H. (2018). Digital forensic challenges in the cloud computing environment. In Recent Trends in Information and Communication Technology (pp. 669–676). Springer International Publishing.

[38] Khanafseh, M., Qatawneh, M., & Almobaideen, W. (2019). 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 : IJACSA, 10(8). https://doi.org/10.14569/ijacsa.2019.0100880

[39] Prasad, K. (2016). Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework. In Proceedings of the 3rd Australian Counter Terrorism Conference (pp. 9–14).

[40] Haeberlen, A. (2010). A case for the accountable cloud. ACM SIGOPS Operating Systems Review, 44(2), 52–57. https://doi.org/10.1145/1773912.1773926

[41] Hargreaves, C., & Patterson, J. (2012). An automated timeline reconstruction approach for digital forensic investigations. Digital Investigation, 9, S69–S79. https://doi.org/10.1016/j.diin.2012.05.006