electronics MDPI

Review

Cloud and Edge Computing-Based Computer Forensics: Challenges and Open Problems

Vijay Prakash [1], Alex Williams [2], Lalit Garg [1,3], Claudio Savaglio [4,*] and Seema Bawa [1]

[1] Department of Computer Science & Engineering, Thapar Institute of Engineering & Technology, Patiala 147001, Punjab, India; vijay.prakash@thapar.edu (V.P.); lalit.garg@um.edu.mt (L.G.); seema@thapar.edu (S.B.)
[2] Computer Science Department, University of Liverpool, Liverpool L69 3GH, UK; lexwill2000@gmail.com,
[3] Computer Information Systems, Faculty of Information & Communication Technology, University of Malta, Msida MSD 2080, Malta
[4] Institute for High Performance Computing and Networking (ICAR), National Research Council, 87036 Rende, Italy
* Correspondence: claudio.savaglio@icar.cnr.it

Abstract: In recent years, there has been a dramatic change in attitude towards computers and the use of computer resources in general. Cloud and Edge computing have emerged as the most widely used technologies, including fog computing and the Internet of Things (IoT). There are several benefits in exploiting Cloud and Edge computing paradigms, such as lower costs and higher efficiency. It provides data computation and storage where data are processed, enables better data control, faster understanding and actions, and continuous operation. However, though these benefits seem to be appealing, their effects on computer forensics are somewhat undesirable. The complexity of the Cloud and Edge environments and their key features present many technical challenges from multiple stakeholders. This paper seeks to establish an in-depth understanding of the impact of Cloud and Edge computing-based environmental factors. Software and hardware tools used in the digital forensic process, forensic methods for handling tampered sound files, hidden files, image files, or images with steganography, etc. The technical/legal challenges and the open design problems (such as distributed maintenance, multitasking and practicality) highlight the various challenges for the digital forensics process.

Keywords: cloud computing; edge computing; computer forensics; digital evidence; forensic software tools; forensic software tools; digital forensic investigation process

check for updates

Citation: Prakash, V.; Williams, A.; Garg, L.; Savaglio, C.; Bawa, S. Cloud and Edge Computing-Based Computer Forensics: Challenges and Open Problems. *Electronics* **2021**, *10*, 1229. https://doi.org/10.3390/electronics10111229

Academic Editor: Pietro Manzoni

Received: 14 April 2021
Accepted: 16 May 2021
Published: 21 May 2021

1. Introduction

Cloud computing has emerged as a ubiquitous technology with new capabilities for the smooth and fast delivery of computer resources such as servers, networks, storage, applications, and services on demand with minimal management requirements [1]. It is also one of the most critical milestones in developing computer systems and technologies that can be integrated and utilized efficiently [2,3]. Cloud computing services are very economical and expandable [4–8].

Recently, Edge computing has created a new construct in the computing environment. It brings Cloud computing services next to the end-users and is defined by faster processing and quick response to the requests. Internet-enabled applications such as real-time traffic monitoring, surveillance, and virtual reality requires prompt response time and faster processing [9]. Edge computing's promising features include mobility support, location awareness, very low delays, and access to users. These features make Edge computing suitable for various future applications in a plethora of domains such as transportation, entertainment, wellness, health, industry, etc. [10–14].

The Cloud computing design is flawless, and its benefits are subject to criminal exploitation [15]. Additionally, the authors of [16–18] argued that this conflict with the traditional digital investigation method creates various law enforcement challenges with digital forensic technology practitioners. Criminals use the Cloud as a safe place to store and hide possible digital evidence [19]. Indeed, the authors of [20,21] discussed that Cloud computing had added new digital forensic investigation requirements. Its design process introduces unique risks related to confidential information, integrity, and the impact of discovery of computer forensics [22]. Cloud and Edge computing's impact on computer forensics is divided into concepts of two separate, but related challenges—technical and legal [23–27].

Data in the Cloud/Edge are primarily flexible, resulting in various technical challenges. One of the most common legal barriers to Cloud/Edge forensics is concerned with legal issues. From the legal viewpoint, these legal challenges are primarily considered as evidence such as authentication, hearsay, chain of custody and preservation [24,28]. In most cases, the Cloud/Edge Service Provider (SP) can obtain the data from various law enforcement authorities. Thus, the data (as evidence) are subject to multiple legal considerations simultaneously. This is especially difficult when there is a third-party SP. In other words, the SP uses the services of another SP located in various locations. If data storage and other services are not included in the SP, issues regarding the actual site of the data and data ownership can confuse the investigation process. There are different rules of evidence in many jurisdictions, and differences in crime and criminal offences are not consistent with some of the many legal issues in various categories.

1.1. Motivation

The purpose of this review paper is to establish a more in-depth understanding of the challenges of Cloud and Edge computing in computer forensics. From the technical viewpoint, these include the difficulty in dealing with various data stored in multiple locations (by authorities), limitations in accessing Cloud/Edge resources that build strong evidence, and maintaining the evidence's integrity [29,30]. Further, large amounts of data in the Cloud/Edge cannot be easily handled and processed without the risk of contamination or damage to the evidence's integrity [31]. The nature of digital evidence compared to physical evidence is complex, requiring a new criminal system to control the collection of digital evidence [32]. Dealing with the massive amount of data distributed across multiple domains has seemed to add to the problem on an ongoing basis [33,34].

1.2. Our Contribution

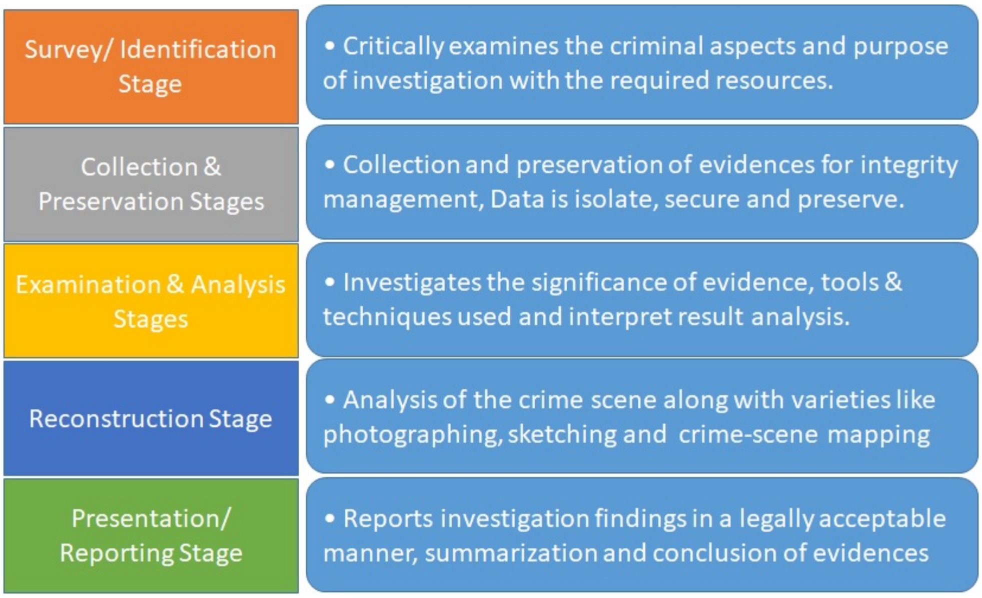
We present a prime review paper that highlights the digital forensic process for both Cloud and Edge computing and its different challenges and open problems. Further, it is the only survey paper that contains the following information at a place:

1. All the hardware and software tools available for the digital forensic process in Cloud and Edge computing;
2. Effect of encryption methods on Cloud/Edge forensic analysis;
3. Basic details of forensic methods for handling tampered sound files, hidden files, image files, or images with steganography (e.g., to protect copyrights).

The rest of the paper is organized as follows. Section 2 describes the literature review. Section 3 presents Edge forensics challenges with Cloud computing and existing solutions. Section 4 discusses the forensic analysis tools, encryption methods and methods for handling different types of files. Section 5 discusses the open problems existing in the related study. Section 6 discusses the nature and scope of the technical and legal challenges, followed by Section 7, which concludes the paper and discusses future work directions.

2. Literature Review

This review process discusses the most acknowledged challenges of Cloud/Edge computing in computer forensics. In some ways, the review is critical in highlighting the limitations and shortcomings of the different solutions proposed. Research gaps have also appeared in other proposals for further review and implementation. For this study, the most common steps used in a digital research model have been taken, as presented by the authors of [28,35]. Where necessary, two or more related stages from other models are put together to give some emphasis and clarity, as shown in Figure 1. The outcome of this review is discussed in the following subsections.



Survey/ Identification Stage	• Critically examines the criminal aspects and purpose of investigation with the required resources.
Collection & Preservation Stages	• Collection and preservation of evidences for integrity management, Data is isolate, secure and preserve.
Examination & Analysis Stages	• Investigates the significance of evidence, tools & techniques used and interpret result analysis.
Reconstruction Stage	• Analysis of the crime scene along with varieties like photographing, sketching and crime-scene mapping
Presentation/ Reporting Stage	• Reports investigation findings in a legally acceptable manner, summarization and conclusion of evidences

Figure 1. Digital forensic investigation process.

2.1. Survey/Identification Stage

This stage involves examining criminal aspects related to crime. This approach is based on the active involvement of the criminal elements(s). This stage recognizes that an incident has occurred from key indicators present in the scene and determines the participation level and its nature [36]. However, the widespread nature of Cloud/Edge computing makes the identification process very difficult. Investigators rarely know about the exact location of evidence. Additionally, the forensic detective has limited access to evidence in the Cloud/Edge and therefore performing any identification encounters significant challenges. Flexible retention that translates into the highest risk of data loss in the physical environment is also a concern [37–39]. A suspect in the Cloud/Edge may choose to restart or turn off the power of VMs and hardware related to the distortion of any available evidence [40]. Therefore, if there is no continuous record-keeping, there will be no identification of evidence or even collection opportunities. When you are in a public Cloud, the identification process becomes much more complicated than a private Cloud [37]. The following are the solutions that exist for the problem.

2.1.1. Log-Based Approach Model

The authors of [41–43] emphasize wood logging for research purposes. In particular, the authors of [42] proposed a separate location log on the client side and then aligned it with the CSP log using unique IDs and timestamps that provide relevant event details. Furthermore, they argued that this approach was designed to simplify digital forensics in computerized environments. However, going back to Sang's suggestion [42] that CSP-controlled information has entered the client's side, it is argued that this limitation ensures comparable data on both sides of the transaction, i.e., the client side and the CSP side. The authors of [43] identify specific security and privacy threats over the SaaS-based

CRM solutions and the measures to overcome them to ensure business processes' smooth functioning.

2.1.2. Access of Evidence in Logs Using a Prepared API

The authors have proposed another solution [5], which identifies partly with Sang [42], in finding potential evidence from the client-side log. Their solution has been compiled as a "Client-Side Evidence Identification Process" that looks at using a pre-configured API that can extract system-appropriate data for both SaaS and PaaS applications. It is said that the process will look at the raw logs and the state of use of the client side. It is therefore limited to information available on the client side only, such as the IaaS model solution. There are no usage indicators for SaaS and PaaS models due to customer access to APIs in these models. Further, the authors of [44] have identified all the aspects of log-based Cloud forensic techniques in the digital investigation process.

2.1.3. Using Eucalyptus Software-Syslog or Snort Logs

The authors of [22] recommended using a standard logging method that ensures timber retention. Using the log management system, the process collects and associates logs containing important information such as the suspect machine's IP address, the type of browser used, and information on the number of HTTP requests and the requested content. This solution has been implemented and validated in the Eucalyptus cloud environment, using analytical tools such as Snort to monitor the Eucalyptus cloud environment's environmental performance.

2.1.4. The Persistent Storage Device for the Client's Data

The authors of [5] have proposed a solution that uses persistent customer data storage for volatile data. While this comes with additional costs, the solution comes with two benefits: firstly, it improves data security and access to data for customers and provides easy access to evidence if a cloud computing force is forced. This proposal's success depends mostly on implementing a global SLA-like policy between the CSP and the client. Another downside to this solution is the client's release of data confidentiality, as the proponents have stated. The SLA means that customer data should be erased entirely at the contract end. To ensure confidentiality, all user data should be encrypted enough to prevent unauthorized reading. The authors of [45] proposed a model to obtain residual data from all activities performed by GDrive users on Android smartphones. Therefore, this proposed approach may assist investigators in obtaining residual data from a GDrive client and may provide information to law enforcement personnel.

2.1.5. An Integrated Conceptual Digital Forensic Framework

For volatile data, the authors of [21] proposed an integrated digital concept framework as a test method for analyzing VMs in the absence of persistent storage. This proposal is based on two widely used digital forensics frameworks [46] and NIST [47]. In addition to this approach, the authors of [48] suggested using a compatible data synchronization model that synchronizes data variables between VM and persistent storage for forensic use. The authors of [49] proposed a model for data collection and forensic Cloud construction, by using feature-based machine learning and prioritization on VMs. The authors proposed a forensic approach for PaaS and SaaS models to design and develop new digital technologies and improve research efficiency and may provide information to law enforcement personnel.

2.2. Collection and Preservation Stages

These stages include the collection and retention of evidence for maintaining integrity and usefulness. Once identified, the evidence has a potential value and should, therefore, be collected and protected from unwanted damages that will make them unreliable, incomplete, infallible and unreliable [50]. This process is challenged in investigations involving the Cloud/Edge partly due to shared features of the Cloud/Edge environment [5,9] and reliance on the CSP to store evidence, making it available to digital investigators. Somehow, CSPs face a series of technical challenges to provide good and fast data [51]. Collection and preservation stages' issues also include Cloud/Edge quality classification (that might be unsuccessful due to high-frequency problems), data reliability, time synchronization, data availability, and the timeline of events in the Cloud directly affecting stock storage [23–25,51]. The following are the available solutions to the problem.

2.2.1. The Trust Model and Trust Cloud

CSP and client/investigator trust relationships are required at the highest level so that CSPs can provide specific information on request [51]. The authors of [52–56] have discussed using multiple layers of trust to allow customers and investigators to gather evidence, including VM images, network logs, processes and information. Both of these solutions seek to address the lack of transparency between CSPs and clients, which is why they build a relationship of trust. However, as the authors of [51] point out, the level of dependence on the control aircraft is essential for the reliability model [53,54]. These solutions are also targeted at IaaS and PaaS models and cannot be successfully implemented in the SaaS model.

2.2.2. Isolation Techniques

The authors of [57] suggested methods and procedures that can be used to differentiate Cloud conditions to prevent contamination and distortion of evidence during collection, thus maintaining authenticity. The solution seeks to address the problems of a significant expansion in the Cloud by separating VM conditions. Their proposed strategies include condition transport, server farming; failover; address delivery; sandboxing; and the middle man. In Cloud forensics, it is used to collect and analyze data between the data exchange process between the model and Cloud hardware, which effectively allows the forensic approach to be performed on all data used by the model without interfering with other conditions. However, the authors of [51] pointed out that these methods were doctrinal and could not be tested or given any kind of experiment.

2.2.3. Secure Provenance Schemes

With the advent of data in the Clouds, the authors [58] proposed a "Secure Provenance Scheme" for Cloud computing that records data objects' identity and processing history in the Cloud. The solution depends on the team's signature and authentic signature strategy, which aims to provide "privacy of sensitive documents and performance of Cloud-based location records", among others. The program addresses two key issues—security and privacy, emphasising who receives what and when. In this way, issues related to child custody [59] and anonymous access are addressed through the "Trusted Evidence Mechanism" solution offered. However, it is not clear whether this program works on all three Cloud models or has limitations. The proposed system's safety has been demonstrated under certain assumptions of it being standard and proven. The authors of [60] proposed a model except for the buyer of the service and the service provider. An additional obligation of the Cloud auditor has been included as the services used by consumers are accessible to all users even if the provider enables login features for each system where the customer has limited access. Suppose a forensic analyst reports an issue. In this case, the investigator will conduct a preliminary investigation by collecting provenance records from the last history and finally prepare a report to be submitted to the court authorities.

2.2.4. The Trust Platform Module (TPM)

Data reliability is an essential requirement for the acceptance of evidence in the courts. The authors of [5,48,53] proposed the use of the Trust Platform Module (TPM), which aims to maintain the confidentiality and integrity of data in the Cloud. The TPM solution provides additional security for authentication, encryption and signing so that evidence can be retained and cannot be criminally altered or removed without notice. However, as the authors of [53] point out, one problem with TPM is that its safety is still in doubt as effective procedures can be modified without detection. Additionally, the implementation of TPM on PaaS and SaaS models is uncertain due to limitations in access to the hypervisor. Moreover, the problem of compatibility with many current devices in the Cloud is troubling, and as a result, CSPs are unlikely to support their implementation. The use of TPM is also not severely tested, and there is no indication of any internal claims.

2.2.5. VM Snapshots

Collecting evidence sometimes requires making a forensic copy (bit-by-bit image) of Cloud storage systems. The authors of [18] suggested using VM Snapshots to help capture and investigate the design of the IaaS model. However, this solution is limited to accessing portable devices in the private delivery model, but not in the public Cloud. Additionally, this solution does not apply to SaaS and PaaS models. In the IaaS model, things are a little different as the client (and the investigators) controls the Cloud infrastructure that includes storage. The authors of [61] improve the migration framework of a secure machine that enables a reliable platform module for many virtual machines operating on the hardware platform while maintaining the integrity of the Cloud system.

2.3. Examination and Analysis Stages

The examination and analysis stages meet undoubtedly to be the most challenging of traditional digital research, particularly the analytical process investigating the value of evidence and its significance for testing [36]. These categories become a significant challenge for cloud forensics due to the scale and increased volume of resources and materials to be tested, in line with the limitations of the processing and testing tools [51]. Additionally, there are limited tools available for performing forensic tests and analysis due to the highly informal cloud data format. It is often understood that traditional forensic tools have various limitations brought about by the diffused and elastic features of the cloud paradigm [39,59]. For example, Encase and FTK (the most widely used forensic tools) cannot be used to retrieve, analyze or test cloud data due to the high level of trust required.

For this reason, the development of applications that translate the traditional cloud data format into something readable and tangible may be necessary. Another option is to develop tools that can be used to test and analyze data in a conventional cloud data format. The following are the available solutions to the problems.

2.3.1. The Offline Windows Analysis and Data Extraction (OWADE) Tool

The (OWADE) tool was developed by the Open-Source Software Foundation, which can retrieve information about the website and the user, has visited, extract data stored in the cloud, disclose user identity, and resume online session activities. This tool is essential because the internet is the gateway to many cloud services and resources, and providing this data will be a crucial step forward in the investigation. However, the authors of [51] have shown that this app is still developing and only works with Windows XP drivers. Meanwhile, Microsoft applications have been continuously upgraded; Windows 10 is the latest version that makes Windows XP less functional.

2.3.2. The Management Plane

The "Management Plane" proposed by [53] is another recommendation that provides a balance between speed and reliance when obtaining and analyzing Cloud-based evidence. This solution is part of the authors' proposals that include the "Platform Modules", "Forensics-as-a-service", and "legal solutions", all of which consider less trust but require more co-operation in the CSP.

2.3.3. The Forensic Open-Stack Tools (FROST)

The authors of [53] developed the FROST, a management plane forensic toolkit for acquiring forensics data from virtual disks, API logs and guest firewall logs.

2.4. Reconstruction Stage

The reconstruction phase in a digital investigation is closely tied to the analysis stage. The data reconstruction process produces a variety of analyses [5]. In other categories, Cloud computing also contributes to the reconstruction phase in several ways. The distributed Cloud-based environment hinders the execution of any brief analysis with a consistent timeline that can be used to re-track the logical sequence of crime events [37]. Following are the solutions that exist for the problem.

LVM2-Based System Snapshots

To rebuild the crime scene, the authors of [62] proposed a solution that duplicated the attack and restored the system to its original state. Their proposed method uses LVM2 System abbreviations to revive the attack event each time a Cloud system attack occurs.

2.5. Presentation/Reporting Stage

The presentation/reporting stage entails reporting investigation findings in a legally acceptable manner [35]. It is the final stage in an analytical investigation where evidence is formally presented in court or by another judicial body [63]. The presentation stage successfully contains a summary of the entire investigation process, and a description of the conclusions [36]. Presenting or reporting the outcome of digital investigations involves using cloud services and applications that face similar challenges and showing the result of traditional digital investigations due to strict legal requirements.

Cloud computing and complexity factors have added to these challenges due to several issues that need to be overcome in the course of a court investigation into the Cloud. In most cases, investigators are required, in their presentations, to explain the procedures used to obtain evidence and how it relates to the case. However, Cloud technologies that include multiple applications, visualization and simultaneous access (to name a few) make the definition very difficult to understand for those with limited technical knowledge. In presenting the investigation findings, the legal investigator, as a professional witness, will have to prove that the evidence was collected using legally permitted methods that are very difficult to follow in the Cloud space. The Cloud's shared and multidimensional features make it challenging to determine where and to whom the crime was committed, let alone determine in what country the case should be brought and where it can be heard [38]. Following are the solutions that exist for the problem.

2.5.1. Seminars and Associate Conferences

Conferences should be held to raise awareness among judges and other legal stakeholders about the complexity of digital investigations involving the Cloud. In addition, court administrators (e.g., judges and magistrates) will need corresponding qualifications to demonstrate their understanding of the basics of Cloud computing and related evidence available in the Cloud.

2.5.2. Repeatable and Reproducible Conclusions

When presenting the findings of an investigation, the investigator should ensure that the results of the analysis should be repeated and redefined by the same or another forensic investigation. This will increase credibility in the report and go beyond the fact of simply presenting a piece of channel-controlled information.

The various previous stages of the case investigation process and the challenges that exist will impact the presentation phase because the previous sections' processes and outcomes are discussed and reported in the presentation section. For this study, the most common steps of a digital research model have been taken, as discussed by the authors of [35]. Where necessary, two or more related steps from other models are put together to give some emphasis and clarity. Table 1 summarizes the recommendations already presented by various authors to address the multiple challenges encountered at different stages of the digital forensics process.

The disadvantages of the methods discussed for the challenges/issues in the digital forensic investigation process have already been highlighted under the "Limitations/Drawbacks" attribute of Table 1. A brief discussion on the advantages and disadvantages of each approach is presented in Table 2.

Table 1. Summary of challenges/issues and existing solutions.

Challenges/Issues	Existing Solutions	Cloud Services Model Applicability			Application Details	Limitations/Drawbacks	Reference(s)
		IaaS	PaaS	SaaS			
Volatile Data	Persistent Storage Framework	✓	✓	x	Enable continuous use of customer data storage	It comes at an added cost; privacy issues; largely depends on the implementation of international policy between the CSP and the client	[5,45]
	Integrated (iterative) conceptual digital forensic framework	✓	✓	x	It uses the live forensic method of testing and analyzing VMs	There is no proof of testing and evaluation	[21,48,49]
	The continuous data synchronization model	✓	✓	x	Continuous Synchronization on API	There is no evidence of any criminal activity	[48,49]
Access to Evidence	Log-based Model	✓	x	x	Uses transaction and event logs	It does not resolve issues related to dynamic data	[41,43]
		x	✓	✓	It uses a separate location log on the client-side aligned with the CSP log using different IDs and timestamps. Additionally, it uses different IDs and timestamps that provide relevant event details	The CSP determines what information is included on the client side	[42,43]
	Log-based Model (Client-Side Evidence Identification Process)	✓	✓	x	Built-in application logs	No proof of implementation or evaluation	[5,42,44]

Table 1. *Cont.*

Challenges/Issues	Existing Solutions	Cloud Services Model Applicability			Application Details	Limitations/Drawbacks	Reference(s)
		IaaS	PaaS	SaaS			
	Standard Logging Mechanism	✓	x	x	It uses the Eucalyptus framework and the standard log security process	N. A	[22]
	Encrypted Logging Model	✓	✓	x	Uses system status and log files	N. A	[48]
CSP Dependency	The proposed framework collects the forensic data outside the cloud to avoid CSP dependency	x	x	x	The proposed framework is validated through Distributed Denial of Service (DDoS) attack	It is used for small prototype models only	[64]
Data Collection	VM Snapshots	✓	x	x	Works by freezing and investigating the system in the IaaS model	This solution is limited to mobile devices' access in the private delivery model but not to public clouds	[18,61]
Data Acquisition: Trust Issues	Trust Model	✓	✓	x	Uses multiple layers of trust	An additional level of reliance is required on the management of aircraft	[53–56]
	Trust cloud	✓	✓	x	Uses multiple layers of trust	An extra level of trust is required in the management plane	[51,53,54]

Table 1. *Cont.*

Challenges/Issues	Existing Solutions	Cloud Services Model Applicability			Application Details	Limitations/Drawbacks	Reference(s)
		IaaS	PaaS	SaaS			
Data Integrity and Chain of Custody	Trust Platform Module	✓	✓	✓	Provides added security for authentication, encryption and signing	Problems with compatibility with most current devices in the cloud. Additionally, some security issues in those operating procedures can be changed without being detected	[5,48,53]
Data Isolation and Multi-tenancy Issues	Isolation Techniques and Procedures	✓	✓	✓	Functions by isolating and separating cloud conditions to prevent contamination and disruption of evidence during collection	The strategies mentioned were strategic, as also presented by Alqahtany et al. (2015), were theoretical and were not tested or under any experiment	[51,57]
Data Provenance	Secure Provenance Scheme	✓	✓	✓	Tasks by recording the identity and processing history of data objects in the cloud and based on group signature and attribute-based techniques	The safety of the proposed system is shown under certain assumptions that they say are commonplace and proven	[58,60]
Chain of Custody	Staff Training	✓	✓	✓	N. A	N. A	[59,60]
Lack of Forensic Tools	Forensic Open-Stack Tools (FROST); Offline Windows Analysis and Data Extraction (OWADE)	✓	✓	x	Management Plane	Works only on drives with Windows XP installed (for OWADE)	[51,53]

Table 1. *Cont.*

Challenges/Issues	Existing Solutions	Cloud Services Model Applicability			Application Details	Limitations/Drawbacks	Reference(s)
		IaaS	PaaS	SaaS			
Data Loss due to Machine Restart	Snapshots	✓	✓	✓	Functions by replaying the event of an attack and restore the system to the state it was before	N. A	[62]
Lack of understanding of cloud complexities and other technical comprehension	Training	N. A	N. A	N. A	N. A	N. A	[38]

Table 2. Advantage/disadvantages of approaches used in the digital investigation forensic process.

Stage	Approach	Advantage	Disadvantage/Limitations
Survey/Identification stage	Enhanced Digital Investigation Process (EIDIP) Model [36]	• Separate the primary and secondary crimes significantly. • Investigation phases are considered iterative instead of linear.	• It is very time-consuming due to the iterative phases of the digital investigation process.
	Cybercrime Forensic Framework [40]	• Considers the collection and preservation stage. • Make multiple images of the relative records and files for primitiveness and integrity of the evidence.	• Highly dependent on FTK and EnCase tools for the forensic analysis. • Performance is not up to the Cloud scale.
	Log-based approach [41]	• Log consumers can process, analyze, and correlate the emitted log records effectively and efficiently	• Not able to handle forensic timeline analysis, log review, log correlation, security visualization and policy monitoring.
	Log-based model [42]	• Check the activities on SaaS cloud without the support of the CSPs. • Create a customized log for both CSCs and CSP.	• Data and logging for multiple users may be co-located with spread hosts and data centres.
	Log-based approach for Cloud CRM [43]	• Time saving for uploading, backup, and maintenance purposes. • Focused on log centralization, log records retention and maintenance and integrity preservation at the same time.	• Not able to handle log management for maintaining big data and large-scale organizations. • Results analysis is possible only after performing live attacks and security requirements for large number of datasets.
	Mobile forensic investigation for Remnant data [45]	• Identification of Remnant data on GDrive data and applications for all CSCs.	• Restricted to GDrive for Android Smartphone only.

Table 2. *Cont.*

Stage	Approach	Advantage	Disadvantage/Limitations
	Snapshot based on Technical and Legal Challenges [21]	• Requires authenticated credentials from users to decrypt the file on the server.	• Restricted to their private cloud-only.
Collection and Preservation stages	Clouds and Edge computing security challenges [51]	• Considered Cloud and Edge as the revolutionary technologies in terms of security, trust and client management.	• Cloud and Edge computing still face several issues with customer-centred privacy, customer authentication system, and customer service level agreement.
	TrustCloud [52]	• Considered Security, Privacy, accountability and suitability as the main trust parameter for the cloud. • Detective rather than preventive approaches to increasing accountability.	• Restricted to logging mechanism for data layer of accountability apart from workflow, system, Policies and Laws and regulations.
	Cloud Forensic Readiness Framework [54]	• Time, money and efforts have been reduced by thorough digital investigation and collection of data before the crime incidence.	• Privacy and forensic techniques were not considered in the initial proposed framework. • Readiness framework has been validated through a single organization only.
	Secure provenance scheme [58]	• Provides provenance tracking on disputed documents, the provenance record's unforgeability, and fine-grained access control on documents. • Sensitive documents stored on the Cloud are confidential and handle the authenticity to Cloud servers anonymously.	• Security of the proposed scheme has been validated through assumptions instead of real-life experimentation.

Table 2. *Cont.*

Stage	Approach	Advantage	Disadvantage/Limitations
	Forensic Enabled Data Provenance Model [60]	• SLA policies, Database architecture, Data logging security, Timestamp and data trust have been considered in a single model.	• NA
	Forensic Investigation using VM Snapshots [18]	• Eucalyptus and OpenStack software is used to capture a snapshot of running VM automatically for evidence collection.	• Only a single VM has been considered at the moment.
	Secure Live Job Migration Framework for multiple VM [61]	• Load balancing, fault management, recovery from host failure, system maintenance and resource sharing have been effectively considered during the VM migration process. • Virtual trusted platform module had been used to provide trusted computing for multiple VM in a single snapshot.	• The integrity of the proposed approach has been verified using various assumptions based on physical access of attacker, VM communication mechanism and virtual trusted platform module.
Examination and Analysis Stages	Pros and cons of digital forensic in Clouds [39]	• Availability of massive storage for evidence in clouds. • Inbuilt mechanism for hash authentication of disk drives	• Data acquisition as the significant issue. • Temporary files, registry entries, and memory may be very difficult to access in cloud data centers.

Table 2. *Cont.*

Stage	**Approach**	**Advantage**	**Disadvantage/Limitations**
Reconstruction stage	Logical Volume Manager 2 (LVM2)-based system snapshot for forensic analysis [62]	• Provide both read-write functionality by default compared to read-only function of LVM1. • Mount the snapshot volume by experimental programs to change files on that volume.	• Threshold values have not been detected correctly.
Presentation/Reporting stage	Digital Forensic Readiness [63]	• It uses remote and centralized logging to improve the authenticity of archived data in order to overcome jurisdictional issues on Clouds.	• The proposed model works for Windows only. • Protect operating system or hypervisor and central log server.

3. Edge Forensics: Challenges with Cloud Forensics and Existing Solutions

Edge computing extends Cloud computing by providing computer services closer to end-users on the Edge of the network. Edge's view addressed the problem of high delays in services sensitive to delays and malicious programs within the Cloud computing paradigm [65]. However, Cloud and Edge computing has established its power and usefulness through features such as low cost, reliability, local sensitivity, wireless communication, and local access. These power features pose new problems in the area of privacy, security, and legal practitioners. There is no doubt that Cloud computing brings many challenges in investigating digital forensics conducted in the Cloud. Given these challenges, it is vital to analyze and understand the impact of Cloud computing on forensic investigation and identify the various methods, tools and techniques used to solve these challenges. We decided to focus on these paradigms (Cloud and Edge) as these technologies' challenges are the almost same.

The authors [26] proposed a log assuring secrecy scheme in Edge-Cloud Environment. In this approach basically investigator is trying to recover the log files as shown in Figure 2, Initially all the users log has been stored on the Edge nodes. Later on the users log after segmentation has been stored to the distributed storage system and centrally located Cloud node. In first phase attacker will try to destroy/steal data for Edge node instead of central storage or distributed storage system. In second phase, attacker will attack on the Cloud node for stealing the data. In between, on suspect the Edge Cloud service provider will talk to investigator to do the investigation on the data and store it. The investigator is able to recover the data from central storage or distributed storage system but not able to recover it from the Edge node destroyed/stolen by the attacker. Further, with the help of MIC network and index files, the data can be finally recovered from the Distributed storage clusters.

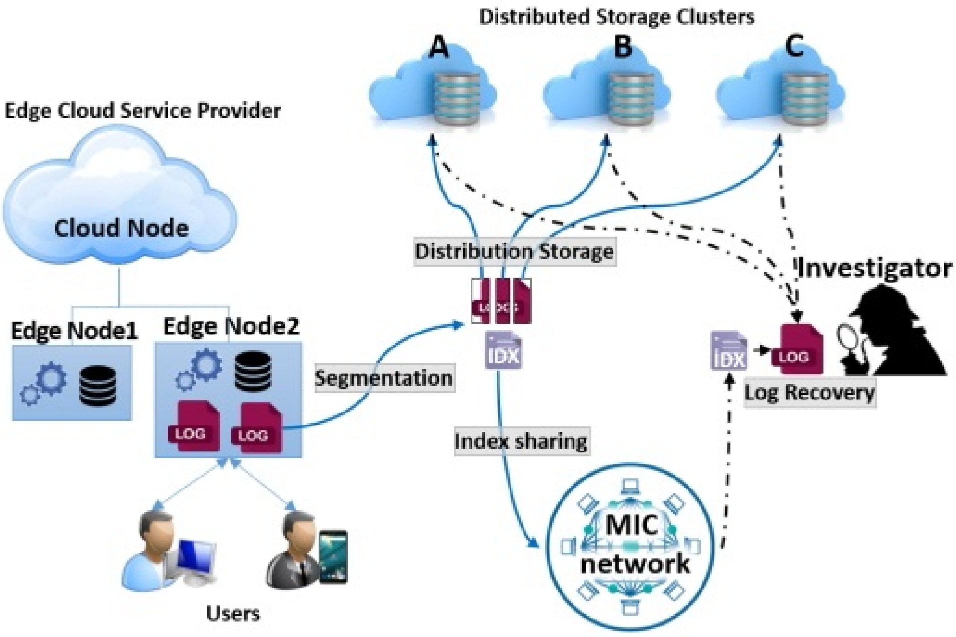


Figure 2. Digital forensic investigation for Edge/Cloud systems. Reproduced from [26].

An essential advantage of connecting the Edge with a computer is achieving great power under high simultaneous access, real-time guarantees, travel support, and data persistence. Cloud computing's elastic storage and extensions capabilities allow us to address the demands of scalability, perseverance, and trust. Edge computing deals with the services hosted on nodes that are held by Internet Service Providers (ISPs), and other smaller servers which are available near users in the network. The Nano Datacenters

(NaDa) [66] model is one of the examples of the current trend of disruption of the Edge of complex network operations that were traditionally performed "Network-centric".

Some of the suggested Cloud computing solutions, such as data integrity schemes, searchable homomorphic encryption, and test data retrieval, can find a limited program on an Cloud/Edge computer due to high data and work migration through the Edge nodes and Cloud [67–69]. Another key security feature is Cloud protection infrastructure from external attacks access control. However, as the Edge nodes are not in a single administrative domain, these nodes might not necessarily be compatible with management authority. Most of the challenges associated with Cloud/Edge forensics have already been summarized in Tables 1 and 2. In addition to having conflicting access control policies, Cloud owners' nodes may need to extend their access management policies by using other trusted third parties places. Such a transfer model may be the case of harassment by an opponent [70].

4. Forensic Analysis: Tools, Encryption and Files Handling Methods

The term "forensics" refers to the methods that investigators use to solve the crime. Each innovation has its benefits as well as drawbacks. The art of investigating a crime is performed or involved with a computer, called computer forensics. Computers and electronic devices are developing very fast and being used in modern crime. Strictly speaking, computer forensic technology can be used to collect and preserve evidence from devices and later introduce it in court. These devices have been developed and can perform all types of operations from essential to advanced levels. The forensic investigator is mainly responsible for the examination and preservation of data evidence. He/she must be aware of the techniques, procedures, and processes of crime evidence.

4.1. Computer Forensic Software Tools

Computer forensic tools are designed to guarantee that the data collected from the computer are precise, accurate and trustworthy. Due to the different types of computer-based evidence, there is a diverse range of computer forensics tools [71]. The well-known open-source and business software tools for digital forensics are tabulated in Table 3. The list consists of their detailed descriptions, characteristics, compatibility with the operating system and website links.

4.2. Hardware Tools for Forensic Analysis in Cloud and Edge Computing

In this section, the various hardware tools/devices used for forensic analysis in Cloud and Edge computing are discussed in detail [70].

4.2.1. Data Recovery Stick

A data recovery stick can recover deleted files quickly from any location, even the files that have been permanently deleted from the recycle bin. The investigator can still retrieve the deleted files until the files' locations are overwritten with new data or not excessive. There is no need for any installation and any other software.

4.2.2. Phone Recovery and iRecovery Stick

The phone recovery stick includes special recovery software on USB drives that allow recovering data on Android-based smartphones and tablets, which can be checked even with a locked screen. It can recover deleted data unless the data have not been overwritten. Similarly, the iRecovery Stick contains special testing and recovery software on USB drives that allows anyone to check data on iPhone- and iPod-based touch devices. Similarly, the iRecovery Stick can also recover deleted data unless overwritten.

Table 3. Software tools for digital forensic analysis in Cloud/Edge environment.

Tool	Description	Features	OS Compatibility	Reference
Pro-discover	It allows investigators to identify and re-allocate data on a computer disk. With the help of this tool the investigator can protect evidence and create quality reports for the use of legal procedures to be presented in the court.	• Extract EXIF (Exclusive Image File Format) data from Joint Photographic Expert Group (JPEG) files. • Quickly search for suspicious files. • To view the internet history. • Makes a copy of the all the suspicious files to back up the actual evidence. • Import or export images in .dd format. • VMware to play the captured image.	Windows, Mac, and Linux	https://www.prodiscover.com (accessed on 6 May 2021)
Sleuth Kit (+Autopsy)	It enables forensic analysis to check the hard drives and smartphones.	• Effectively locate activity using a graphical interface. • Collect records from logs, SMS, contacts, etc. • Path and name decides the flag of files and folders • Tag files with random tag names. • Images are displayed with their thumbnails • Provides e-mail analytics. • Group files to search all documents or images by type.	Windows and Linux	https://www.sleuthkit.org (accessed on 6 May 2021)

Table 3. *Cont.*

Tool	Description	Features	OS Compatibility	Reference
FTK Imager	It can make several data copies without altering the actual evidence. This tool allows investigators to stipulate benchmarks to reduce extraneous data such as file size, pixel size and data type.	• Developed by AccessData • Supports pre- and post-processing improvements. • Cybercrime can be detected using wizard-driven approach • Helps the investigator to maintain reusable profiles for various test needs. • Retrieve passwords from more than 100 applications.	Windows only	https://accessdata.com/products-services/forensic-toolkit-ftk (accessed on 6 May 2021)
Magnet RAM Capture	With the help of Magnet Ram Capture the investigators can retrieve and analyze valuable objects identified in the memory by capturing the memory of the suspicious computer.	• Can execute while minimizing overwritten data in extraneous memory. • Export the extracted memory data and upload it to diagnostic tools such as Magnet AXIOM and Magnet IEF.	Windows only	https://www.magnetforensics.com (accessed on 6 May 2021)
CAINE	This tool can be integrated as a module into existing software tools. Further, with the help of CAINE, forensic investigator captures the timeline from RAM automatically.	• Supports the digital checker in the four out of five stages of the digital investigation process model. • Provides a user-friendly interface as well as user-friendly tools. • Can be customized.	Linux only	https://www.caine-live.net (accessed on 6 May 2021)

Table 3. *Cont.*

Tool	Description	Features	OS Compatibility	Reference
X-Ways Forensic	Forensic investigator can use this tool to support disk cloning and imaging. Further, it allows the investigators to collaborate for the joint forensic with other peers from their group having the same tool.	• Automatically detects lost or deleted partitions. • Read partitions and file system within .dd image files. • Analyze remote computers. • Provides written protection to maintain data authentication. • Use disks, Redundant arrays of independent disks (RAID), etc. • Easily detect New Technology File System (NTFS) and Alternative Data Stream (ADS). • Supports bookmarks or annotations. • View and edit binary data using the template.	Windows only	http://www.x-ways.net/forensics/ (accessed on 6 May 2021)
Registry Recon	Forensic investigator can use this tool to extract, retrieve, and analyze registry information and data from Windows Operating systems. This program is helpful for effectively determining the external devices connected to any PC.	• Rebuilds the active registry database. • All volume shadow copies (VSCs) can be mounted quickly on disk. • Automatically retrieves valuable NTFS data. • Easily connectable to the Microsoft Disk Manager utility tool.	Windows only	https://arsenalrecon.com/products/ (accessed on 7 May 2021)

Table 3. *Cont.*

Tool	Description	Features	OS Compatibility	Reference
PALADIN	This digital forensic software provides over 100 valuable tools to investigate any malicious content. It allows investigators to simplify the range of forensic tasks.	• More than 33 categories that can help investigators to complete the task. • Offers both 32-bit and 64-bit versions. • Available on a USB thumb drive. • Toolbox includes open source tools to help investigators to easily find the required information.	Windows and Linux only	https://sumuri.com/software/paladin/ (accessed on 7 May 2021)
Volatility Framework	Forensic investigators use this tool to check the runtime state of a system using data exist in RAM. It is a Software for Volatility Framework, Memory Analysis and Digital Forensics.	• API that allows investigators to view Page Table Entry (PTE) flags quickly. • Investigators can collaborate with their peers with same software installation. • Provides several plugins to check MAC file operations. • Supports Kernel Address Space Layout Randomization (KASLR). • Service executes the fail-over command automatically when a service fails to start multiple times.	Windows, Mac OS X, and Linux	https://www.volatilityfoundation.org (accessed on 7 May 2021)
e-Fencer	It allows investigators to search for files from any device in a simple interface. Further, also helps investigators to meet computer forensics and cybersecurity needs	• Capture memory, Internet history, and screen from the system on the USB thumb drive. • Supports multithreading. • Protects against malicious behavior, hacking and policy violations.	Windows, Mac OS X, and Linux	http://www.e-fense.com/products.php (accessed on 7 May 2021)

Table 3. *Cont.*

Tool	Description	Features	OS Compatibility	Reference
EnCase	It helps investigators to retrieve credentials from the hard drive. It allows investigators to analyze files in depth to gather evidence such as documents and pictures, etc.	• Thoroughly diagnose treatment (severity and priority of diagnoses) • Acquires data from many devices including mobile phones, tablets, laptops and desktops, etc. • Automate the production of evidence. • Quickly search, locate and prioritize evidence. • Used to unlock encrypted evidence. • Allows generating complete reports to protect the integrity of the evidence.	Windows only	https://www.guidancesoftware.com/encase-forensic (accessed on 7 May 2021)
Crowdstrike	It can provide threat intelligence, endpoint protection and more. The forensic investigator can quickly discover and resolve cybersecurity incidents and prevent attackers in real- time.	• Back up a physical, virtual and Cloud-based data centre. • Manage system errors. • Automatically detect malware.	Windows and Mac only	https://www.crowdstrike.com/endpoint-security-products/falcon-endpoint-protection-pro/ (accessed on 7 May 2021)
Xplico	It supports Internet Message Access Protocol (IMAP), Hypertext Transfer Protocol (HTTP), and other relevant networking protocols. There is no limits on number of files and no size restrictions on data entries.	• Real-time support. • Output data into SQLite database or MySQL database. • Reserve DNS search from DNS packages containing input files. • Provides Port Protocol Identification (PPI) feature to support digital forensics. • Open source but supports both IPv4 and IPv6.	Linux only	https://www.xplico.org (accessed on 7 May 2021)

Table 3. *Cont.*

Tool	Description	Features	OS Compatibility	Reference
Wireshark	It is used for network testing, troubleshooting and to check the various traffics going through computer system by analyzing network packets.	• Output can be exported to Extensible Markup Language (XML), Comma Separated Values (CSV) file or plain text. • Reads live data from the network, Bluetooth, ATM and USB, etc. • Compressed files with GZip which can be quickly decomposed. • Provides rich Voice over Internet Protocol (VoIP) analysis. • Allows investigators to read or write a file in any format. • Decryption support for multiple protocols, including Internet Protocol Security (IPsec), Secure Sockets Layer (SSL) and Wired Equivalent Privacy (WEP).	Windows, Mac OS X, and Linux	https://www.wireshark.org (accessed on 7 May 2021)
SANS SIFT	It provides digital forensics and event response testing facility on based on distribution tool of ubuntu. It can automatically update the DFIR (Digital Forensics and Event Response) package.	• Can be installed through the SIFT-command-line interface (CLI) installer. • Make better use of memory. • Contains latest forensic tools and techniques.	Windows, Mac OS X, and Linux	https://digital-forensics.sans.org/community/downloads/ (accessed on 6 May 2021)

4.2.3. Project-A-Phone Flex

Project-A-Phone Flex can take high-quality screenshots of any device. The eight-megapixel camera allows the investigator to take clear pictures of each screen on the device to miss nothing. It is an easy way to test a flex cell phone when the investigator does not have software. The camera connects appropriately to the investigator's computer to acquire clear images of the cell phone pictures. The investigator can also record HD quality videos of the entire testing procedure.

4.2.4. Chatstick

Chatstick covers the entire computer with Yahoo, MSN 6.1, 6.2, 7.0, and 7.5, ICQ 1999–2003b, Trillion, Skype, Hello, and Miranda, etc. It scans for all these chatboxes and creates a report in a simple format so that investigator can see what their relatives, friends or employees are saying to people online.

4.2.5. Forensic Ultradox Right Blocker V5.5

Digital and forensic investigators, technicians and lawyers who want to safely view, evaluate, or depict a disk drive based on CRU, WiebeTech, etc., can opt for Forensic Ultradox v5.5. It is an easy-to-use, professional-class drive dock that provides a stock of hosts and drives connections to recover and analyze the delated or malfunctioned data.

4.2.6. Dp2c

It is a powerful and compatible tool with built-in data-target triage and a complete disk-imaging tool. Investigators can collect specific data objects such as graphics or documents and e-mails, etc. This tool is bootable, easy to use and provides all the functionality required by an investigator to collect the data.

4.2.7. Mobile Field Kit

It includes the Project-a-Phone in a licensed and robust, portable case of the DS embedded on the Windows laptop, cable and power options. The main advantage of MFK is that it uses an open system, which allows investigators to place other mobile forensics or computer forensic software on your system for use in the field. The investigator has the choice of a standard Windows laptop or a ruggedized laptop. This allows manual driver updates to support most new phones without having to wait for a software update. Further, MFK, a handheld cellular exploit device with a device capture driver embedded in the hardware, was used. The hardware comes in a rugged case and has a touchscreen capability for the mobile extraction unit. MFK allows logical and physical acquisition of handheld/mobile devices with built-in capabilities.

4.2.8. Strong Holdbags and Tabletop

Strong Holdbags are used to block signals from wireless networks, signal sources that can threaten digital evidence and cell towers, etc. However, it does not permit incoming communications to alter the evidence or send a wiping order. Similarly, another popular tool called Tabletop Stronghold tents can block wireless signals from wireless networks, cell towers, and other signal sources.

4.2.9. Forensic Duplicator

Forensic Duplicator integrates multiple devices into one simple unit for better performance. Field units combine forensic imaging applications (Linux) quickly and easily with virtual drive emulators and S.M.A.T diagnostic tests. This is used as a platform to perform: cellphone/tablet data extraction and analysis, complete computer forensic analysis and forensic triage data collection. It is particularly fast with E01/Ex01 formats, runs at full compression, and uses multiple threads in multiple sessions. Forensic duplicator units are available with a dual boot option.

4.3. Effects of Encryption Methods on Cloud Forensic Analysis

Applications running on the Cloud can balance various factors, including data size, bandwidth, load balancing, and security. The main obstacles to Cloud reception are privacy and data security because data owners and CSPs are not within the same trusted domain [72]. A series of different technologies or cybersecurity algorithms are used to protect and maintain privacy in Clouds. These techniques mainly include encryption, limited service and strict access, data backup, and facilitate data recovery [73]. To ensure security and data privacy from a Cloud service provider, an encryption mechanism must encrypt the data before uploading them to the server.

The key technique is public-key encryption based on the public key cryptographic algorithms. In traditional public-key algorithms/techniques, the data owner encrypts the data with the user's public key before uploading it to the Cloud. When a data user wants to access the data in the Cloud, then the Cloud provides a related cipher/private key for encrypted data. The user then decrypts this cybertext with the private key. Attribute-based encryption (ABE) [74] is a new invention that works using one to many relations and is also called fuzzy encryption.

The authors of [75] have discussed the encrypted search mechanism in Cloud storage, as shown in Figure 3. Both the data owners and data users need to follow the different search methods. Data owners can store their data files using encryption and index files corresponding to the encryption algorithm. This encrypted file and the index file can be stored in the Cloud storage system. The person or data user having the decryption key/algorithm can only retrieve and access the original file shared by the data owner. In this case, if an attacker is trying to access the encrypted file, he/she must have the relevant decryption key or algorithm either shared by the data owner or CSP.

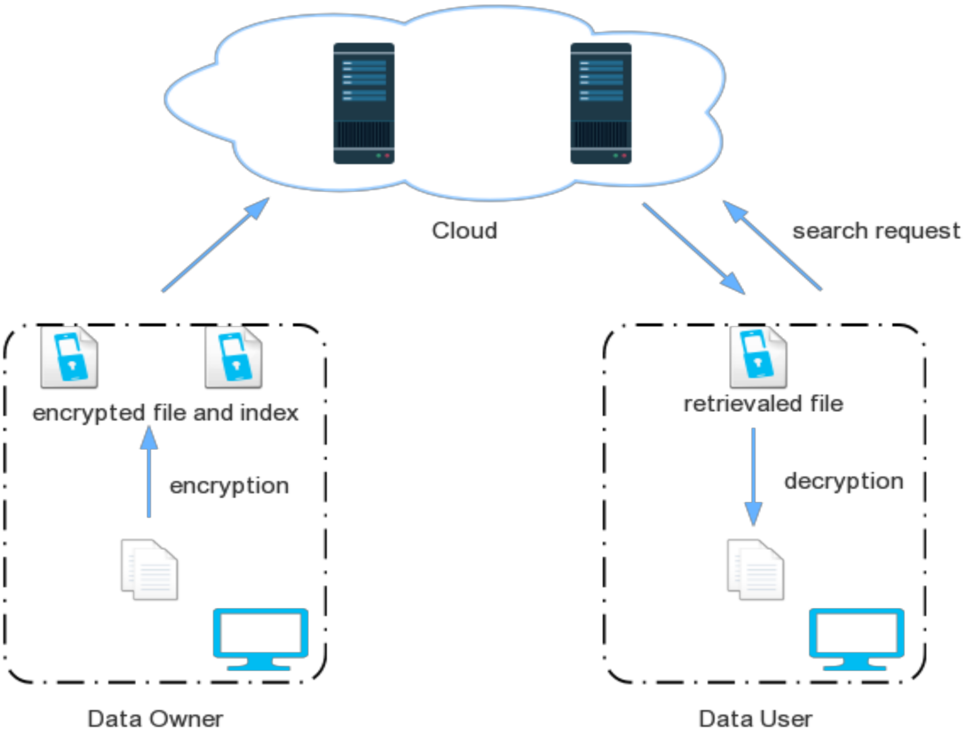


Figure 3. Encrypted search in Cloud storage. Reproduced from [75].

Android is one of the leading smartphone operating systems globally, and it is essential to know about Android forensics. In addition, chat messaging is becoming a popular medium of communication among consumers, especially young people. The authors of [76] had extensively analyzed encrypted instant messaging (IM) applications such as Whatsapp, Viber, Telegram and WeChat, etc. The primary purpose of studying the forensic analysis of these applications is to encrypt the database and media files. Data availability is of key interest to law enforcement agencies for acquisition and analysis. Sometimes database of these applications in encrypted form can be provided by forensic investigators. However, in some cases, the encryption key may be available in the application itself. They make extensive use of popular instant messaging applications for encrypted and secured chat database files.

The encrypted archived files for Viber and WeChat can be downloaded from a rooted handset. The WeChat database can be decrypted with the encryption key provided by the IMEI number and the phone's unique identifier. Further, WhatsApp messages can be retrieved from unrooted devices. Additionally, archive files for WeChat can also be collected from an unrooted device by degrading it to a lower version to the existing version. Telegrams is the most secure IM applications compared to all the others. Even if the database files are retrieved, the encrypted chat database files cannot be decrypted without the encryption key [76].

Forensic investigators are primarily concerned with the security and privacy of sensitive e-mail data. Encrypted e-mail seems to be a feasible option for providing security but is limited to its considerable operational functionality. Public encryption with the Keyword Search (PEKS) is a popular scheme [77] with regard to the combined security and friendly operation functions, which play an essential role in finding encrypted e-mail on the Cloud server.

The author of [78] proposed "public-key multikeyword searchable encryption with hidden structures" (PMSEHS) with public-key multikeyword searched encryption. It enables e-mail receivers to conduct multikeyword and Boolean searches on massive encrypted e-mail databases without disclosing any additional data to the Cloud server. The author of [79] explores the potential for retrieving remnant data residues for preliminary research for criminal investigations that may be carried out for pCloud software. It is based on a study in volatile memory. In pCloud, Investigator can download, import, and open files in the Cloud in three different ways. pCloud is a kind of private Cloud computing designed specifically for file storage. It simply depicts the interaction in terms of a user-friendly app and how it works. It is available for smartphones and computer systems as it has several operations on operating systems such as Mac OS X, iOS, Android, Windows and Linux. It is installed on top of a local disk space system on a stable virtual drive called pCloud. It is used to create tools.

The author of [80] proposed "forward-secure puncturable identity-based encryption" (fs-PIBE), which allows the e-mail user to indicate the decryption capability accurately. The user will be allowed to conserve the decryption capability of the unencrypted e-mail and remove the received ones. Therefore, it allows more practical forwarding confidentiality than specific etiquette, in which the decryption capability of received and unpublished encrypted e-mails is simultaneously withdrawn. With a consistent fs-PIBE construct, constant ciphertext, and proven encryption in a standard format, the authors create the appearance of an encrypted Cloud e-mail system and speed it up. Furthermore, the authors extended the proposed fs-PIBE system to enable end-to-end encryption and outsource decryption to improve the protection and reliability of the proposed mechanism.

4.4. Forensic Methods for Handling Tampered Sound Files

Audio forensics refers to assessing and investigating audio recordings for accurate confirmation of genuineness of any audio evidence in court. Audio forensic algorithms are used to prove the audio evidence's authenticity, improve speech transparency and lower-level sound's audibility, improve audio recording and documentation. In addition, it can be used to identify the speaker, clarify the conversation, and understand audio evidence, such as crime or accident scenes [81]. The lack of widely accessible forensic datasets for performance assessment and benchmarking and modern multimedia forensic algorithms is one of the challenges in multimedia forensics.

High-quality audio playback system, waveform display system, and spectrographic display system are the primary instruments in modern audio forensic research. Standard desktop or notebook computers are typically used to complete these functions [82]. External non-audio knowledge about a problem, suspects, circumstances, and the investigator's suspicions are often sources of prejudice in audio forensic examinations. An individual demanding an audio forensic investigation would wish to discuss the accused's arrest history, explain the physical evidence found at the crime scene, and refer to the requested finding as a "case". Typically, an audio forensic investigation begins with a request from a law enforcement agent or an attorney. It is possible that the applicant is not acquainted with audio forensics techniques.

It is highly recommended to start with the original recording medium and, if possible, make certified digital work copies and any improvement or commentary work before beginning the interpretation recording system. The original recording system may allow investigators to retrieve specific original proprietary data, device settings, metadata and other recording settings, timestamps, etc. If the device has special connectors, cables, and power supply, these also need to be requested. Some recording devices may have volatile memories: the recorded signal is lost if the power is lost. This should be taken into account to ensure that the memory is protected from potential power loss. Some storage systems have volatile memories, which means that the signal is lost if the power goes out. This step should be taken to ensure that the memory is safe from power outages. The sender should be asked to back up the proof with the "Written protection" mode and other mechanically overwritten preventive settings.

Recordings are always subject to accidental changes or intentional tampering, and these changes may not be noticeable. The court must have confidence in the audio evidence's accuracy and integrity. Audio forensic examiners should observe chain-of-custody protocols, avoid allowing for unanticipated improvements in the actual evidence, and be aware of signs of alteration.

The authors of [83] developed a digital audio forensic data collection to help analyze audio forensic algorithms. They included data-gathering environments, cameras, speakers, languages, and notation in detail. Established tamper detection devices use artefacts caused by recording instruments, codecs, and acoustic settings. The audio portion of the reference audio is replaced with an audio recording recorded with a related microphone in the same recording session to create the manipulated audio dataset. The collected dataset is used to detect damage to the audio data file. This study examines the inter-range spread of microphone artwork. The recordings of five different microphone models would be regarded in this respect. It is important to note that each microphone category has at least two similar microphones and versions [83].

The authors of [84] proposed a new paradigm for emerging multimedia data processing approaches for multiple multimedia sources. They focused on speeches, videos and pictures, handwriting and text. The toolkit forms the methods and techniques for gathering information from multiple multimedia sources that can be used in various contexts in court. Additionally, social media such as Twitter and Facebook allow multimedia data in new formats to the data described above. The referenced data can further be provided to the investigators for coincidence and variations, including more symbolic features based on individuals, biometric features or objects, events or data features.

Transient techniques such as spectral, delta modulation, wavelet scattering, and zero-crossing information are used to develop speech and audio representation schemes. For example, traditional and structural similarity-based methods: example-based voice, speaker, and audio recognition can compare aspect and overall similarity using query-based, keyword, and phrase-based retrieval schemes. The resulting scheme is both computationally simpler and data compression effectively.

The author of [85] considers a method to verify speech recording instead of a two-step reference: align the two recordings and then classify each question frame as matching or mismatched. Furthermore, the proposed sub-sequence alignment method is based on the Needleman–Wunsch algorithm and proves that it improves the dynamic time when performing simple manipulation operations. In addition, the authors explore several binary taxonomic models based on LSTM and transformer architectures to verify content material at the frame level. Through extensive experiments on Donald Trump's speech recording, they reliably explored the various types and periods of audio tampering activity.

4.5. Forensic Methods for Handling Image Files

Multimedia files play a crucial role in supporting evidence analysis to assess crime by viewing files as digital guides or evidence. Traditional file recovery software detects and reconstructs parts of a file using markers such as titles and footers. The Joint Photographic Experts Group (JPEG) file data format is widely used in computers, mobile phones, the Internet, multimedia applications, and digital cameras due to its advanced features [86]. File recovery is the process of recovering deleted or damaged files from digital storage when file metadata are available [87].

Digital forensics is the application of file retrieval methods on bit-copy images of disk drives. It emphasizes retrieval and preservation of different parts of the assigned data and is different to the investigation. The authors of [88] adopt engraving techniques as a base work due to its comprehensive approach to retrieving JPEG files. The accuracy and authenticity of a digital image are often challenging to visualize due to the advent of advanced image processing and manipulation techniques. Various digital image forensics approaches have been proposed over the last decade to detect digital image forgery.

The authors of [89] provide a brief overview of passive digital image forensics methods to provide a broad innovation to recent digital image forensic security advances. Various traces can be used in digital image forensics to differentiate manipulated images from natural ones. Furthermore, the authors divided these traces into three categories: traces leftover from image acquisition, traces leftover from image storage, and traces leftover from image editing. For each trace, the relevant digital image forensics approach is briefly reviewed by clarifying the relevant issues.

The authors of [90] proposed a model for efficiently and accurately identifying the forensic process by classifying bulk JPEG images generated by the data engraving process or other means. JPEG images with errors or corrupted data fall into the first classification. JPEG images with lattice fields fall into the second classification, and JPEG images without corrupt or forgery codes fall into the third. Furthermore, the proposed model would automatically allow investigators to automatically label JPEG images, minimizing the amount of time spent on the whole digital forensic procedure.

Locating the source of multimedia data, i.e., identifying the model, make, or personal computer that will capture the media material is a common problem in forensic analysis. As opposed to sensor noise-based approaches, source linkage allows for more direct automation based on media element header detail. The header detail consists of metadata such as Exchangeable image file format (EXIF) tags and JPEG algorithm parameterization.

The authors of [91] researched the factors affecting the metadata and the JPEG-encoder based on the sources of the images taken by Apple's iPhone cameras. The diversity of image metadata requirements is greatly enhanced as compared to the ecosystem of conventional cameras. Source device identification is even more difficult in the case of traditional digital cameras. The authors demonstrated the whole process in four stages. First, the dataset collected from Flickr contained more than fifty thousand images from an Apple device. Second, the EXIF metadata of the smartphone on Apple devices will change over time. Third, the change is less integrated with the original Apple hardware, but the iPhone operating system is more associated with the version change in iOS. Finally, automatic taxonomy training outperforms hardware platforms in evaluating iOS models.

The author of [92] used a Convolutional Neutral Network (CNN) to decide on which images were tempered and look for image irregularities such as identical patches of pixels. This dataset, in particular, includes duplicate images created using the copy-move technique. The authors mainly focus on different types of image-manipulated analysis methods such as:

1. Detecting traces of resampling;
2. Splicing detection based on inconsistencies in geometry perspective;
3. Analysis of noise inconsistencies;
4. Splicing detection based on lighting/shadows;
5. Enhancement detection;
6. Cyclostationary analysis;
7. Seam carving detection.

Copy-move forgery is a form of image tampering in which a portion of an image is copied and pasted onto another, usually to mask unsightly data. The aim of determining each transmission type is to locate picture regions that are identical or very similar. Such characteristics (e.g., noise and colour) are consistent with the rest of the image if the copied bits are from the same image. This means that forensic approaches that look for statistical inequalities will not detect such an attack.

The authors of [93] suggested a part-level middle-out learning technique for structurally efficient classification to detect dual compression. The authors first show that single and double compressed data with different JPEG coder settings will form a limited number of coherent clusters in a featured space representation. They also visualized the behavior of several well-known Benford-based functions. Finally, in the feature engineering family, the proposed model was used for the double JPEG compression detection problem. When compared to similar strategies in this family, the proposed approach has less complexity but a comparable efficiency.

4.6. Forensic Methods for Handling Image Files with Steganography

Steganalysis and steganography are two distinct techniques of cybersecurity or digital investigation. Steganography seeks to hide messages from the naked eye, while steganalysis aims to confirm their existence or retrieve embedded data. Steganography and steganalysis have recently received a lot of media attention, mainly because they have been used by law enforcement. It is an old technique derived from the Greek terms steganos (cover) and graph (writing). Since cryptography is prohibited or forbidden by law in many countries, hiding messages is very popular these days [94]. Steganography is the process of hiding a message, audio, image or video by embedding it in another picture, audio, news or video. Therefore, understanding how messages can be embedded in a digital medium, such as digital images. Over the years, many robust and powerful methods of steganography and steganalysis have been demonstrated in the literature.

The author of [94] used various steganography techniques to identify confidential data in digital images. Steganography is commonly used for watermarking and fingerprinting to protect Intellectual Property Rights (IPR). The watermark is embedded in the host statistics not to be deleted without causing damage to the host media. An invisible data monogram on a watermarked object documents the actual owner of the data to validate copyright protection [95]. In practice, all digital file formats are marked with steganography with a distinctive mark of redundancy.

Many practical steganography applications enhance the power of image search engines and smart identity cards and include information from people embedded in their photographs and content under copyright control. Other important applications include television transmissions, video audio synchronization, secure movement of corporate confidential information and TCP/IP protocol packets. Specific data are embedded in the image for perseverance to check the network traffic of specific handlers. JSteg [96], F5 [97], Outguess [98], MB [99], YASS [100] are the major JPEG stenographer approaches. In addition, the authors of [95] classify stenographic systems, which convert image documents into invisible data into the following categories.

1. Spatial Domain Steganographic Systems [101];
2. Statistical Procedures [102];

3. Image Frequency Domain Steganographic Scheme [103];
4. Distortion Methods [104];
5. Dossier Embedding Method;
6. Palette Embedding;
7. Image Generation Method;
8. Image Element Adjustment Methods;
9. Adaptive Steganography;
10. Spread Spectrum Image Steganography (SSIS) Technique.

Without understanding the steganographic algorithm, Stego can be extracted using essential image processing functions in an anti-forensic way. The authors of [105] proposed the Persistent Stego Incident Response System (PSIRS) anti-stego algorithm, which is used to make images and videos without stego without affecting critical visual quality. The authors use a combination of different algorithms, such as RS algorithms [106] and Universal Steganalysis [107]. Peak Signal-to-Noise Ratio (PSNR) and Structured Similarity Index Measure (SSIM) are used to evaluate the quality of clean images and videos. PSIRS can remove up to 80% of the stego without affecting the visual appearance and video quality. The authors of [108] analyzed cutting-edge techniques for steganography and steganalysis. The authors have identified various areas/applications that can use steganography in real life.

1. Military personnel use steganography as a general means of communication for confidential communication;
2. National Security Agencies (NSAs) use steganography to transmit confidential messages inside and outside the agency;
3. Hiding the details of the people in their photo in the smart ID;
4. Since unreliable communication may often lead to serious data loss, corporate and industry communication is monitored for protection and authenticity;
5. Watermarking is used for copyright information notation;
6. Advanced data structure;
7. Document tracking tools;
8. Electronic money;
9. Radar system and remote sensing;
10. Multimodal biometric data, etc.;
11. Medical science uses image steganography in medical images used for diagnoses such as CT and MRI.

There are many examples of criminals and terrorists using steganography for communication. Here are some examples from the real world

1. U.S. officials and several articles claim that al-Qaeda used steganography to plan the “9/11 attacks” [109]. Later in 2012, an al-Qaeda member was arrested in Berlin with a chip that contains video files containing steganography.
2. “Operation Twins” is an international paedophile racket known as the “Shadow Brotherhood” [110].
3. The University of Purdue reported that several computers had been found with information relating to financial fraud and a device that hides data with child pornography [111].
4. The Federal Bureau of Investigation (FBI) states that 10 Russian goosebumps in the United States are using stenography and that confidential data have been leaked to Moscow from the United States [112].

A good steganography technique or equipment must meet the basic requirements of the steganography system, including aptitude, efficiency, visibility and safety. In addition, there are reversibility, encryption, computational complexity and other requirements for better technology. Multimedia, archives, networks, Skype, medical videos, and DNA are some of the latest steganography patterns [108]. The author of [113] demonstrates the classification of steganography based on technical and non-technical steganography.

Different types of linguistic and technical steganography are discussed. Subsequently, PSNR, MSE, robustness, and the domain insert technique evaluate the output of other image stereography methods. Many of the current algorithms have some benefits and drawbacks. The latest steganography has also been integrated into detail with the embedding algorithm and the extraction process. In some steganography algorithms, data hiding and payload capabilities distort embedded data and the original image. Different algorithms have different payload capabilities. It is now essential to develop an efficient and effective infrastructure that provides the high-payload ability, data embedding and restoration without distortion, improved protection and accuracy, and attacker resistance technology.

5. Open Problems

The literature review covers the challenges that various authors and the proposed solutions have already been identified to address them in detail. However, some challenges were identified as open problems as they still needed to be addressed or required real-life solutions. These issues, as discussed by the authors, are:

1. “Reliance on CSPs” to obtain information as evidence in the Cloud [51];
2. Critical time issues and data analysis from multiple sources and compilation of evidence from various distribution agencies [51];
3. Reconstruction of crime in the cloud [51];
4. “Overcoming border crossings” as a result of the spread of cloud computing [51];
5. “Lack of system control” means that evidence cannot be held for preservation [51];
6. “Jury’s technical understanding” limits the judges’ jurisdiction and in addition the court’s understanding of the Cloud technology and complexity and hence the changing face of the evidence [51];
7. Data acquisition is concerned with knowing where the data are and receiving the data [38,39];
8. Registry entries, temporary files, and memory may be difficult when cloud data centers are impossible to access due to virtualization [38,39];
9. Cybercrime is carried out without regard to time or place. Information services or customer data may be disseminated across many sites or even continents. As a result, it creates procedural ambiguity and controversy in the government’s information security oversight and lengthens the forensic time and complicates the process. Furthermore, judicial questions relating to users’ physical limits are hazy due to virtualized technology, and they must not be overlooked [40];
10. Crime modes can cover various realms, from electronic communities, pornography websites, phishing, copyright piracy, and e-commerce bills, depending on the Cloud network. When sensitive information is destroyed or disrupted legally or by some other medium, privacy problems arise [40];
11. Electronic data include network evidence. The majority of documentation, such as Cloud storage log sheets, email logs of e-commerce bills, or digital signatures. When evaluated and tested by specific authentication, these various types of proof cannot mean anything by themselves. Since electronic evidence is easily tampered with, it is critical to prevent the different factors that compromise the legal impact of the three types of forensic evidence mentioned above [41];
12. How to keep logs as security and synchronized and effectiveness as evidence [42];
13. Improper activities at the network, client and server-end [43];
14. Distributed Denial of Services (DDoS) and Malware Attacks [43];
15. Dependencies due to service providers [43];
16. In the public Cloud deployment model, consumers do not have physical access to the infrastructure, and their data privacy is much lower than those in the private cloud [54];
17. Client computers in Cloud environments can provide minimal evidence due to the storage of real data on the CSP side [54];

18. Timestamp matching of different file system activities during the investigation can be complex as clients and Cloud storage servers may reside in different time zones [54].

Added to these challenges associated with encryption and other security measures by Cloud users to protect the data and communications in the Cloud discussed [114] make it difficult for investigators to clarify details and reconstruct the crime. This study's main aim is to highlight the different technical and legal challenges along with open problems. Further, the study highlights the various software and hardware tools for digital forensics in Cloud/Edge Environment and different file handling techniques related to forensic analysis.

6. Nature and Scope of Challenges: Technical and Legal

Traditional methods of digital forensic investigation are not compatible with computer features. In various ways, they are different and seem to contradict each other—the challenges are apparent and concise. These challenges are broadly classified as technical and legal challenges [23–27].

6.1. Technical Challenges

6.1.1. The Distributive Nature and Volume of Data in the Cloud/Edge Computing

Some of the known challenges of making digital forensics in the Cloud/Edge are: (1) difficulty in dealing with a variety of data stored in various locations (by authorities), (2) limitations in accessing Cloud/Edge resources that build strong evidence, (3) maintaining the integrity of evidence, (4) the volume of data in the Cloud/Edge cannot be easily controlled and processed without the risk of contamination or damage to the authenticity of the evidence, etc. In itself, the nature of digital evidence is compared to that of complex physical evidence, which requires a New Criminal Procedure to regulate the collection of digital evidence [26,32].

6.1.2. Cloud Computing Operational Characteristics

Features of using Cloud computing such as multiuse and sharing, visualization, accessibility, and network distribution have created new forensic investigation challenges. For example, the Cloud's shared environment and the widespread use of visual technology have brought new challenges, especially at various digital road investigation processes' stages, which has become very tedious and impossible. The type of Cloud computing based on remote storage technology, multidisciplinary technology and virtualization technology makes it difficult to forensic research using traditional tools and methods [115]. The scope of Cloud computing resources enabled by virtualization technology [116,117] have introduced many complexities and requirements in the Cloud response space. This includes new requirements for virtual visualizations and vice versa and tracking multiple areas of the operating system [52]. Dealing with the impossible amount of data distributed across multiple domains has been seen to complicate the problem regularly. Additionally, the data in the Cloud are primarily flexible, resulting in a variety of technical challenges.

6.1.3. Nature of Cloud- and Edge-Based Evidence

By its nature, digital evidence is fragile and can be easily altered or destroyed if mismanaged [118]. The dynamic nature of digital evidence in the Cloud/Edge has compounded these problems by bringing new challenges. Cloud/Edge systems by design are often live and active, which brings about issues related to data emergence and real-time reporting issues [52].

6.1.4. Identifying Cloud Suspects

The complexity of the work associated with the Clouds' features has identified the real suspects within the Cloud space as a daunting task; non-disclosure of evidence (such as computers, etc.) could bind the suspect to testimony.

6.1.5. Encryption and Other Security Issues

As customer data can reside in unspecified locations, many organizations use high-encryption applications to protect their data within the Cloud [75,114]. However, this approach also poses significant challenges to intelligence investigators where such data become part of a broader investigation or are considered evidence. The development of encryption techniques makes it difficult for technical investigators to clarify details and reconstruct crime incidents.

6.1.6. Cloud Service Models—Challenges

Different types of Cloud provisioning pose additional challenges to crime investigations. These challenges vary depending on service infrastructure and the environment. PaaS and SaaS are quite challenging due to the unique architecture and complex architecture and complexity in many ways than those of the traditional computer model. On the other hand, the IaaS model has some forensic capabilities as its operating environment is logical and similar to that of the conventional computer environment [37,119]. Therefore, the traditional research method is not possible within the PaaS and SaaS models, where there is an opportunity for the IaaS model [120]. The technical challenges and their implications are summarized in Table 4.

The above challenges are mainly concerned with the general impact of Cloud/Edge computing/features on computer forensics. In a way, the different types of Cloud services present the various challenges and opportunities for digital forensic investigation, as summarized in Table 5.

From Table 5, it is clear that there are many technical and physical barriers to digital forensics in the Cloud/Edge. Some of these barriers, such as proffer, can be remedied using existing forensic tools and processes differently. Others will require the construction of new structures and implementation. At all times, Cloud/Edge forensics also faces legal challenges, which they may encounter in border investigations.

Table 4. Cloud forensics: technical challenges.

Design Parameter	Challenges
Distributed Nature and Remote Storage [26,32]	Establishes location and data identification as part of the investigation process. Additionally, identifying Cloud suspects and taking evidence as part of the preservation process is not possible.
Elastic Storage and Volume of Data [118]	The scale, size, and size of Cloud penetration affect data collection and identification. Additionally, time constraints can identify interest data; there has been a danger of tampering with or undermining the evidence's authenticity.
Volatile Storage [5,45]	There is no guarantee that relevant data can be obtained if required.
Volatile Data [5,45]	Data changes are permanent and thus can be easily destroyed; issues related to data emergence and real-time accountability.
Multitenancy/Sharing and Virtualization [115–117]	Challenges by separating data and related evidence without affecting other clients/users.
Security Obstacles Encryption [75,114]	High encryption and high levels of security are difficult to understand and/or pass.

Table 5. Cloud service models and associated challenges [37,119,120].

Cloud Service Model	Opportunities	Challenges
IaaS	• Traditional forensic detection may work • Abridged VM image can include a cache or act as captured images • Strategically located and easily available so that network access data can be accessed and verified. • Customer-side information is more likely to be a last resort or a transaction • The simplest of all three types	• Live forensics and flexible data access may not be possible • Acquisition images can not include data remnants or unallocated disk space since storage is logical and centered on reserved space. • Hardware not found, failed or obsolete • Multitenant storage devices have the potential to contaminate the procurement process. • Login can be shared collaboratively or distributed across multiple devices and switches • the acquisition will necessitate a significant amount of bandwidth to be completed on time • Data fragmentation and dispersal • Ment Data classification and distribution • Issues of data identity—what happens when the agreement is terminated?
PaaS	• Customer-side forensics are more likely • The forensic approach for web servers or virtualized operating systems (OS) can be used.	• The setting in which investigator log in is determined by the CSP (system calls may not work in CSP) • Systems that are most environmentally friendly.
SaaS	• Availability of application/certification logs is possible • Customer-side information is more likely to be a last resort or a transaction • SaaS application features can help with network forensics • CSP stand-alone equipment contains basic access information.	• It is very doubtful that the conventional acquisition will happen. • CSP controls logging and log data. • It is possible that the details would not work for all Application Programming Interfaces (API) • It is possible that other CSPs are involved. • The implementation of CSPs can be complicated and difficult to study, if not impossible. • Process application isolation • Environmentally sustainable systems are used.

6.2. Legal Challenges

6.2.1. Jurisdictional Issues

One of the most common Cloud/Edge forensics legal barriers is concerned with jurisdictional issues. Other legal challenges are primarily considered in evidence, such as Authentication, Hearing, Chain of Custody, and Preservation. In many cases, the CSP can be found in various legal fields. Therefore, the data (as evidence) are subject to many legal considerations simultaneously. This is especially difficult when there is a third-party CSP—in other words, the CSP uses other CSP services in various locations [121]. If data storage and other services are not included in the CSP, issues regarding the actual location of the data and data ownership may interfere with further investigation. For this reason, the author of [122] argued that the Cloud universe's existence presents unique legal challenges for Cloud researchers. Additional evidence in many private domains, various law breaches, and criminal cases and regulations are inconsistent with some of the many legal barriers to a legal investigation.

6.2.2. Lack of International Collaboration

The challenges posed by legal issues are compounded mainly by the lack of international cooperation between the various authorities involved in the investigation. In some cases, there is a significant lack of legal mechanisms for "access to and exchange of data within the country" and "Lack of legislation/regulation and legal advice", both affecting SLAs and the forensic data collection process [121]. The lack of a coherent legal framework for all authorities makes it impossible to clearly define CSP obligations when it comes to cross-border investigations involving the use of their services. The circumstances under which CSPs can comply with applicable laws and industry standards may vary. Moreover, the lack of law and order in some jurisdictions creates opportunities for legal disputes. It makes it difficult for investigators to follow evidence hidden in the Cloud without a valid reason. Therefore, the forensic data collection process can also be prevented as there are no legal frameworks to enforce or assist forensic investigations.

6.2.3. The Requirement for Seizing Evidence (Admissibility of the Evidence)

Acceptance of evidence is a critical requirement in a court of law. As a result, evidence obtained illegally or without the required consent may provide inconclusive evidence [35]. The process of finding or retrieving evidence usually requires a search warrant. To see it, investigators must make sure that a crime has been committed, that evidence exists, and there is a high probability that there is room for probation. When working with Cloud evidence, achieving these needs is a challenge, mainly due to legal restrictions created by legal issues. Researchers face several difficulties in understanding how digital evidence can change depending on the Cloud service used [121]. Additionally, a forensic investigator may face more significant legal challenges when he or she finds evidence in the Cloud of public prosecution or other acts than when gathering such evidence of criminal prosecution [122]. The forensic investigator can be charged with a criminal offence if the evidence is obtained illegally and without proper examination of official signs.

6.2.4. Paid Service That Requires Protecting Customer Privacy

Cloud computing services mainly come with a limited-service feature [123] and metering capabilities that separate them from free programs and services, including Gmail, Yahoo and LinkedIn. As a result, confidentiality and other legal issues are often discussed and agreed upon in the SLA between the CSP and the client (Choo, 2014). Cloud service buyers who pay for such services will not subscribe to any agreement that will give third-party access to their information in the Cloud or to investigate to disclose information that may affect them or damage their reputation. Some of the most common challenges are summarized in Table 6.

Table 6. Cloud forensic: legal challenges.

Challenge	Impact(s)
Lack of International Collaboration/Jurisdictional Issues, james2015practical, choo2014legal	It affects the timely arrest and detention of witnesses and suspects living/living abroad.
Evidentiary Considerations: Admissibility; Authentication; Hearsay; Chain of Custody; and Preservation, casey2011digital, james2015practical, choo2014legal	Certain legal requirements regarding the taking of evidence and maintaining their integrity are very difficult to meet due to Cloud characteristics.
'Paid Service', snaith2011emergency	Being a customer of the "paid service" Cloud would be counterproductive to approving any SLA that promotes third-party access to their data for intelligence purposes.

7. Conclusions and Future Scope

Cloud and Edge computing have paramount importance in the landscape of computer paradigms. While Cloud and Edge computing are finding great success in medium-sized businesses and large organizational structures, these paradigms pose particular issues for computer forensics. The use of computers technology has already been discontinued. The advent of Cloud/Edge computing has led to new technological and legal challenges that were not common in the traditional computing environment. This study has been conducted on Cloud/Edge computing systems and created a revolution in conventional computer forensic by highlighting all the related challenges and proposed solutions altogether. The primary objective of this study has been to establish a deeper understanding of Cloud/Edge computing's impact on computer forensics. The key findings have been that the impact of Cloud/Edge computing at various stages of the research process is different. Further, this study highlights the detailed description of all the hardware and software tools available for the digital forensic process in Cloud and Edge computing. Effect of encryption methods on Cloud/Edge forensic analysis along with the brief introduction to cryptography. Basic details of forensic methods for handling tampered sound files, hidden files, image files, or images with steganography have also been incorporated to enhance the technical strength of the study. Central to this is understanding of the effectiveness and efficiency of traditional digital technologies at various stages of the research process. The following points are indicated for further, and future research aimed to identify unforeseen challenges and to recognize solutions, where possible:

- Identification of social/cultural barriers to achieve a new framework/model and assess the implications for its conduct and implementation;
- Development of new Cloud/Edge forensics tools based on a new understanding of the concept of challenges and different hardware and software tools discussed in this study;
- Establishment of a standard and internationally recognized toolbar with reliability and guaranteed performance by focusing on reducing or preventing opportunities for investigators who produce results and evidence that provides a plan without finding the truth;
- Creation of a conducive environment for building trust between SPs and clients, especially about what is being recorded for future use (i.e., ongoing maintenance) as investigations arise;
- Assessing the feasibility of the "Location Register" from an ISP or data network providers.

Author Contributions: V.P. worked on the ideas, preparation, creation and/or presentation of the published work, specifically the critical review, commentary or revision—including pre- or post-publication stages. The second author, A.W., worked on the ideas, formulation or evolution of

overarching research goals and aims of the manuscript. The other authors C.S., L.G. and S.B. have played the role of supervisors with oversight and leadership responsibilities for the planning and execution of the research activity, including mentorship external to the core team. Further, they provided valuable suggestions, specifically on the critical review, commentary or revision—including pre- or post-publication stages. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mell, P.; Grance, T. The NIST Definition of Cloud Computing. 2011. Available online: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf (accessed on 15 March 2021).
2. Bhardwaj, A.K.; Garg, L.; Garg, A.; Gajpal, Y. E-Learning during COVID-19 Outbreak: Cloud Computing Adoption in Indian Public Universities. *Comput. Mater. Cont.* **2021**, *66*. [CrossRef]
3. Njenga, K.; Garg, L.; Bhardwaj, A.K.; Prakash, V.; Bawa, S. The cloud computing adoption in higher learning institutions in Kenya: Hindering factors and recommendations for the way forward. *Telemat. Inform.* **2019**, *38*, 225–246. [CrossRef]
4. Anwar, U.; Umair, H.A.; Sikander, A.; Abedin, Z.U. Government cloud adoption and architecture. In Proceedings of the 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 30–31 January 2019; pp. 1–8.
5. Damshenas, M.; Dehghantanha, A.; Mahmoud, R.; bin Shamsuddin, S. Forensics investigation challenges in cloud computing environments. In Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, Malaysia, 26–28 June 2012; pp. 190–194.
6. Sharma, P.K.; Kaushik, P.S.; Agarwal, P.; Jain, P.; Agarwal, S.; Dixit, K. Issues and challenges of data security in a cloud computing environment. In Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 19–21 October 2017; pp. 560–566.
7. Fortino, G.; Russo, W.; Savaglio, C.; Viroli, M.; Zhou, M. Opportunistic cyberphysical services: A novel paradigm for the future Internet of Things. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 Febuary 2018; pp. 488–492.
8. Cole, T.; Bhardwaj, A.K.; Garg, L.; Shrivastava, D.P. Investigation into Cloud Computing Adoption within the Hedge Fund Industry. *J. Cases Inf. Technol. (JCIT)* **2019**, *21*, 1–25. [CrossRef]
9. Khan, W.Z.; Ahmed, E.; Hakak, S.; Yaqoob, I.; Ahmed, A. Edge computing: A survey. *Future Gener. Comput. Syst.* **2019**, *97*, 219–235. [CrossRef]
10. Satyanarayanan, M. The emergence of edge computing. *Computer* **2017**, *50*, 30–39. [CrossRef]
11. Ai, Y.; Peng, M.; Zhang, K. Edge computing technologies for Internet of Things: A primer. *Digit. Commun. Netw.* **2018**, *4*, 77–86. [CrossRef]
12. Liu, D.; Yan, Z.; Ding, W.; Atiquzzaman, M. A survey on secure data analytics in edge computing. *IEEE Internet Things J.* **2019**, *6*, 4946–4967. [CrossRef]
13. Fortino, G.; Messina, F.; Rosaci, D.; Sarné, G.M.; Savaglio, C. A trust-based team formation framework for mobile intelligence in smart factories. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6133–6142. [CrossRef]
14. Aloi, G.; Fortino, G.; Gravina, R.; Pace, P.; Savaglio, C. Simulation-driven platform for Edge-based AAL systems. *IEEE J. Sel. Areas Commun.* **2020**, *39*, 446–462. [CrossRef]
15. Biggs, S.; Vidalis, S. Cloud computing: The impact on digital forensic investigations. In Proceedings of the 2009 International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 9–12 November 2009; pp. 1–6.
16. Daryabar, F.; Dehghantanha, A.; Udzir, N.I.; bin Shamsuddin, S.; Norouzizadeh, F. A survey about impacts of cloud computing on digital forensics. *Int. J.-Cyber-Secur. Digit. Forensics* **2013**, *2*, 77–95.
17. Ab Rahman, N.H.; Glisson, W.B.; Yang, Y.; Choo, K.K.R. Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Comput.* **2016**, *3*, 50–59. [CrossRef]
18. Rani, D.R.; Geethakumari, G. An efficient approach to forensic investigation in cloud using VM snapshots. In Proceedings of the 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 8–10 January 2015; pp. 1–5.
19. Husain, M.S.; Khan, M.Z. *Critical Concepts, Standards, and Techniques in Cyber Forensics*; IGI Global: Hershey, PA, USA, 2019.
20. Martini, B.; Choo, K.K.R. An integrated conceptual digital forensic framework for cloud computing. *Digit. Investig.* **2012**, *9*, 71–80. [CrossRef]
21. Martini, B.; Choo, K.K.R. Cloud forensic technical challenges and solutions: A snapshot. *IEEE Cloud Comput.* **2014**, *1*, 20–25. [CrossRef]
22. Anwar, F.; Anwar, Z. Digital forensics for eucalyptus. In Proceedings of the 2011 Frontiers of Information Technology, Islamabad, Pakistan, 19–21 December 2011; pp. 110–116.
23. AlMendah, O.M.; Alzahrani, S.M. Cloud and Edge Computing Security Challenges, Demands, Known Threats, and Vulnerabilities. *Acad. J. Res. Sci. Pub.* **2021**, in press.

24. Manral, B.; Somani, G.; Choo, K.K.R.; Conti, M.; Gaur, M.S. A systematic survey on cloud forensics challenges, solutions, and future directions. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–38. [CrossRef]
25. Yassin, W.; Abdollah, M.F.; Ahmad, R.; Yunos, Z.; Ariffin, A. Cloud Forensic Challenges and Recommendations: A Review. *OIC-CERT J. Cyber Secur.* **2020**, *2*, 19–29.
26. Park, J.; Huh, E.N. eCLASS: Edge-cloud-log assuring-secrecy scheme for digital forensics. *Symmetry* **2019**, *11*, 1192. [CrossRef]
27. Xiao, Y.; Jia, Y.; Liu, C.; Cheng, X.; Yu, J.; Lv, W. Edge computing security: State of the art and challenges. *Proc. IEEE* **2019**, *107*, 1608–1631. [CrossRef]
28. Chen, L.; Takabi, H.; Le-Khac, N.A. *Security, Privacy, and Digital Forensics in the Cloud*; John Wiley & Sons: Hoboken, NJ, USA, 2019.
29. Fernandes, R.; Colaco, R.M.; Shetty, S.; Moorthy, R. A New Era of Digital Forensics in the form of Cloud Forensics: A Review. In Proceedings of the 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 15–17 July 2020; pp. 422–427.
30. Yaqoob, I.; Hashem, I.A.T.; Ahmed, A.; Kazmi, S.A.; Hong, C.S. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Gener. Comput. Syst.* **2019**, *92*, 265–275. [CrossRef]
31. Amato, F.; Cozzolino, G.; Moscato, V.; Moscato, F. Analyse digital forensic evidences through a semantic-based methodology and NLP techniques. *Future Gener. Comput. Syst.* **2019**, *98*, 297–307. [CrossRef]
32. Kerr, O.S. Digital evidence and the new criminal procedure. *Colum. L. Rev.* **2005**, *105*, 279.
33. Hariri, R.H.; Fredericks, E.M.; Bowers, K.M. Uncertainty in big data analytics: Survey, opportunities, and challenges. *J. Big Data* **2019**, *6*, 1–16. [CrossRef]
34. Jan, B.; Farman, H.; Khan, M.; Imran, M.; Islam, I.U.; Ahmad, A.; Ali, S.; Jeon, G. Deep learning in big data analytics: A comparative study. *Comput. Electr. Eng.* **2019**, *75*, 275–287. [CrossRef]
35. Casey, E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*; Academic Press: Cambridge, MA, USA, 2011.
36. Baryamureeba, V.; Tushabe, F. The enhanced digital investigation process model. In Proceedings of the Digital Forensic Research Conference (DFRWS 2004), Baltimore, MD, USA, 11–13 August 2004.
37. Guo, H.; Jin, B.; Shang, T. Forensic investigations in cloud environments. In Proceedings of the 2012 International Conference on Computer Science and Information Processing (CSIP), Xi'an, China, 24–26 August 2012; pp. 248–251.
38. Reilly, D.; Wren, C.; Berry, T. Cloud computing: Forensic challenges for law enforcement. In Proceedings of the 2010 International Conference for Internet Technology and Secured Transactions, London, UK, 8–11 November 2010; pp. 1–7.
39. Reilly, D.; Wren, C.; Berry, T. Cloud computing: Pros and cons for computer forensic investigations. *Int. J. Multimed. Image Process. (IJMIP)* **2011**, *1*, 26–34. [CrossRef]
40. Yan, C. Cybercrime forensic system in cloud computing. In Proceedings of the 2011 International Conference on IEEE Image Analysis and Signal Processing (IASP), Wuhan, China, 21–23 October 2011; pp. 612–615.
41. Marty, R. Cloud application logging for forensics. In Proceedings of the 2011 ACM Symposium on Applied Computing, Taichung, Taiwan, 21–24 March 2011; pp.178–184.
42. Sang, T. A log based approach to make digital forensics easier on cloud computing. In Proceedings of the 2013 Third International Conference on Intelligent System Design and Engineering Applications, Hong Kong, China, 16–18 January 2013; pp. 91–94.
43. Patidar, M.; Bansal, P. Log-Based Approach for Security Implementation in Cloud CRM's. In *Data, Engineering and Applications*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 33–43.
44. Santra, P.; Roy, A.; Midya, S.; Majumder, K.; Phadikar, S. Log-Based Cloud Forensic Techniques: A Comparative Study. In *Networking Communication and Data Knowledge Engineering*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 49–59.
45. Satrya, G.B.; Shin, S.Y. Proposed method for mobile forensics investigation analysis of remnant data on Google Drive client. *J. Internet Technol.* **2018**, *19*, 1741–1751.
46. McKemmish, R. *What Is Forensic Computing?* Australian Institute of Criminology Canberra: Canberra, Australia, 1999.
47. Kent, K.; Chevalier, S.; Grance, T.; Dang, H. Guide to integrating forensic techniques into incident response. *NIST Spec. Publ.* **2006**, *10*, 800–886.
48. Birk, D.; Wegener, C. Technical issues of forensic investigations in cloud computing environments. In Proceedings of the 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA, 26 March 2011; pp. 1–10.
49. Khan, Y.; Varma, S. Development and Design Strategies of Evidence Collection Framework in Cloud Environment. In *Social Networking and Computational Intelligence*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 27–37.
50. Jiang, K.; Xuan, R. Book Review: Guide to computer forensics and investigations. *J. Digit. Forensics Secur. Law.* **2008**, *3*, 5. [CrossRef]
51. Alqahtany, S.; Clarke, N.; Furnell, S.; Reich, C. Cloud forensics: A review of challenges, solutions and open problems. In Proceedings of the 2015 International Conference on Cloud Computing (ICCC), Riyadh, Saudi Arabia, 26–29 April 2015; pp. 1–9.
52. Ko, R.K.; Jagadpramana, P.; Mowbray, M.; Pearson, S.; Kirchberg, M.; Liang, Q.; Lee, B.S. TrustCloud: A framework for accountability and trust in cloud computing. In Proceedings of the 2011 IEEE World Congress on Services, Washington, DC, USA, 4–9 July 2011; pp. 584–588.

53. Dykstra, J.; Sherman, A.T. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digit. Investig.* **2012**, *9*, S90–S98. [CrossRef]
54. Alenezi, A.; Atlam, H.F.; Wills, G.B. Experts reviews of a cloud forensic readiness framework for organizations. *J. Cloud Comput.* **2019**, *8*, 1–14. [CrossRef]
55. Khan, M.N.A.; Ullah, S.W.; Khan, A.R.; Khan, K. Analysis of digital investigation techniques in cloud computing paradigm. *Int. J.-Next-Gener. Comput.* **2018**, *9*. [CrossRef]
56. Chiregi, M.; Navimipour, N.J. A comprehensive study of the trust evaluation mechanisms in the cloud computing. *J. Serv. Sci. Res.* **2017**, *9*, 1–30. [CrossRef]
57. Delport, W.; Köhn, M.; Olivier, M.S. Isolating a Cloud Instance for a Digital Forensic Investigation. In Proceedings of the Information Security South Africa Conference (ISSA 2011), Johannesburg, South Africa, 15–17 August 2011.
58. Li, J.; Chen, X.; Huang, Q.; Wong, D.S. Digital provenance: Enabling secure data forensics in cloud computing. *Future Gener. Comput. Syst.* **2014**, *37*, 259–266. [CrossRef]
59. Grispos, G.; Storer, T.; Glisson, W.B. Calm before the storm: The challenges of cloud computing in digital forensics. *Int. J. Digit. Crime Forensics (IJDCF)* **2012**, *4*, 28–48. [CrossRef]
60. Haque, S.; Atkison, T. A forensic enabled data provenance model for public cloud. *J. Digit. Forensics Secur. Law.* **2018**, *13*, 7. [CrossRef]
61. Deylami, H.; Gutierrez, J.; Sinha, R. More Than Old Wine in New Bottles: A Secure Live Virtual Machine Job Migration Framework for Cloud Systems Integrity. In Proceedings of the 2018 Eleventh International Conference on Mobile Computing and Ubiquitous Network (ICMU), Auckland, New Zealand, 5–8 October 2018; pp. 1–8.
62. Geethakumari, G.; Belorkar, A. Regenerating cloud attack scenarios using LVM2 based system snapshots for forensic analysis. *Int. J. Cloud Comput. Serv. Sci.* **2012**, *1*, 134. [CrossRef]
63. Trenwith, P.M.; Venter, H.S. Digital forensic readiness in the cloud. In Proceedings of the 2013 Information Security for South Africa, Johannesburg, South Africa, 14–16 August 2013; pp. 1–5.
64. Alex, M.E.; Kishore, R. Forensics framework for cloud computing. *Comput. Electr. Eng.* **2017**, *60*, 193–205. [CrossRef]
65. Zhang, Z.; Zhang, W.; Tseng, F.H. Satellite mobile edge computing: Improving QoS of high-speed satellite-terrestrial networks using edge computing techniques. *IEEE Netw.* **2019**, *33*, 70–76. [CrossRef]
66. Valancius, V.; Laoutaris, N.; Massoulié, L.; Diot, C.; Rodriguez, P. Greening the internet with nano data centers. In Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, Roma, Italy, 1–4 December 2009; pp. 37–48.
67. Atayero, A.A.; Feyisetan, O. Security issues in cloud computing: The potentials of homomorphic encryption. *J. Emerg. Trends Comput. Inf. Sci.* **2011**, *2*, 546–552.
68. Li, Y.; Yu, Y.; Min, G.; Susilo, W.; Ni, J.; Choo, K.K.R. Fuzzy identity-based data integrity auditing for reliable cloud storage systems. *IEEE Trans. Dependable Secur. Comput.* **2017**, *16*, 72–83. [CrossRef]
69. Zafar, F.; Khan, A.; Malik, S.U.R.; Ahmed, M.; Anjum, A.; Khan, M.I.; Javed, N.; Alam, M.; Jamil, F. A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. *Comput. Secur.* **2017**, *65*, 29–49. [CrossRef]
70. Esposito, C.; Castiglione, A.; Pop, F.; Choo, K.K.R. Challenges of connecting edge and cloud computing: A security and forensic perspective. *IEEE Cloud Comput.* **2017**, *4*, 13–17. [CrossRef]
71. Arthur, K.K.; Venter, H.S. An Investigation into Computer Forensic Tools. In Proceedings of the ISSA 2004 Enabling Tomorrow Conference, Midrand, South Africa, 30 June–1 July 2004; pp. 1–11.
72. Balamurugan, B.; Krishna, P.V. Extensive survey on usage of attribute based encryption in cloud. *J. Emerg. Technol. Web Intell.* **2014**, *6*, 263–272.
73. Shabir, M.Y.; Iqbal, A.; Mahmood, Z.; Ghafoor, A. Analysis of classical encryption techniques in cloud computing. *Tsinghua Sci. Technol.* **2016**, *21*, 102–113. [CrossRef]
74. Punithasurya, K.; Priya, S.J. Analysis of different access control mechanism in cloud. *Int. J. Appl. Inf. Syst.* **2012**, *4*, 34–39.
75. Guo, Y.; Liu, F.; Cai, Z.; Xiao, N.; Zhao, Z. Edge-based efficient search over encrypted data mobile cloud storage. *Sensors* **2018**, *18*, 1189. [CrossRef]
76. Rathi, K.; Karabiyik, U.; Aderibigbe, T.; Chi, H. Forensic analysis of encrypted instant messaging applications on Android. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–6.
77. Boneh, D.; Di Crescenzo, G.; Ostrovsky, R.; Persiano, G. Public key encryption with keyword search. In *International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 506–522.
78. Xu, P.; Tang, S.; Xu, P.; Wu, Q.; Hu, H.; Susilo, W. Practical multi-keyword and boolean search over encrypted e-mail in cloud server. *IEEE Trans. Serv. Comput.* **2019**, doi:10.1109/TSC.2019.2903502.
79. Ahmad, N.H.; Hamid, A.S.S.A.; Shahidan, N.S.S.; Ariffin, K.A.Z. Cloud Forensic Analysis on pCloud: From Volatile Memory Perspectives. In *International Conference for Emerging Technologies in Computing*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 3–15.
80. Wei, J.; Chen, X.; Wang, J.; Hu, X.; Ma, J. Enabling (End-to-End) Encrypted Cloud Emails With Practical Forward Secrecy. *IEEE Trans. Dependable Secur. Comput.* **2021**. [CrossRef]
81. Garfinkel, S.L. Digital forensics research: The next 10 years. *Digit. Investig.* **2010**, *7*, S64–S73. [CrossRef]

82. Maher, R.C. *Principles of Forensic Audio Analysis*; Springer: Berlin/Heidelberg, Germany, 2018.
83. Khan, M.K.; Zakariah, M.; Malik, H.; Choo, K.K.R. A novel audio forensic data-set for digital multimedia forensics. *Aust. J. Forensic Sci.* **2018**, *50*, 525–542. [CrossRef]
84. Perner, P. Novel Methods for Forensic Multimedia Data Analysis: Part II. In *Digital Forensic Science*; IntechOpen: Rijeka, Croatia, 2020.
85. Shan, M.; Tsai, T. A Cross-Verification Approach for Protecting World Leaders from Fake and Tampered Audio. *arXiv* **2020**, arXiv:2010.12173.
86. Singh, A.; Jindal, N.; Singh, K. A review on digital image forensics. In Proceedings of the International Conference on Signal Processing (ICSP 2016), Melmaruvathur, India, 7–9 November 2016.
87. Garfinkel, S.L. Carving contiguous and fragmented files with fast object validation. *Digit. Investig.* **2007**, *4*, 2–12. [CrossRef]
88. Ali, R.R.; Mohamad, K.M.; Jamel, S.; Khalid, S.K.A. A review of digital forensics methods for JPEG file carving. *J. Theor. Appl. Inf. Technol.* **2018**, *96*, 5841–5856.
89. Lin, X.; Li, J.H.; Wang, S.L.; Cheng, F.; Huang, X.S. Recent advances in passive digital image security forensics: A brief review. *Engineering* **2018**, *4*, 29–39. [CrossRef]
90. Alherbawi, N.; Shukur, Z.; Sulaiman, R. JPEG image classification in digital forensic via DCT coefficient analysis. *Multimed. Tools Appl.* **2018**, *77*, 12805–12835. [CrossRef]
91. Mullan, P.; Riess, C.; Freiling, F. Forensic source identification using JPEG image headers: The case of smartphones. *Digit. Investig.* **2019**, *28*, S68–S76. [CrossRef]
92. Silaparasetty, V. *Deep Learning Projects Using TensorFlow 2*; Springer: Berlin/Heidelberg, Germany, 2020.
93. Taimori, A.; Razzazi, F.; Behrad, A.; Ahmadi, A.; Babaie-Zadeh, M. A part-level learning strategy for JPEG image recompression detection. *Multimed. Tools Appl.* **2021**, *80*, 12235–12247. [CrossRef]
94. Karampidis, K.; Kavallieratou, E.; Papadourakis, G. A review of image steganalysis techniques for digital forensics. *J. Inf. Secur. Appl.* **2018**, *40*, 217–235. [CrossRef]
95. Yahya, A. *Steganography Techniques for Digital Images*; Springer: Berlin/Heidelberg, Germany, 2019.
96. Johnson, N.F.; Katzenbeisser, S. A survey of steganographic techniques. In *Information Hiding*. 2000; pp. 43–78. Available online: https://www.researchgate.net/publication/245096254_A_survey_of_steganographic_techniques (accessed on 28 April 2021).
97. Steganalysis, H.C.D.B.; Westfeld, A. F5—A steganographic algorithm. In Proceedings of the Information Hiding: 4th International Workshop, Pittsburgh, PA, USA, 25–27 April 2001; pp. 289–302.
98. Provos, N. Defending Against Statistical Steganalysis. In Proceedings of the Usenix Security Symposium, Washington, DC, USA, 13–17 August 2001; pp. 323–336.
99. Sallee, P. Model-based steganography. In *International Workshop on Digital Watermarking*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 154–167.
100. Solanki, K.; Sarkar, A.; Manjunath, B. YASS: Yet another steganographic scheme that resists blind steganalysis. In *International Workshop on Information Hiding*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 16–31.
101. Abdulwahedand, M.N.; Mustafa, S.; Rahim, M.S.M. Image Spatial Domain Steganography: A study of Performance Evaluation Parameters. In Proceedings of the 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET), Shah Alam, Malaysia, 7 October 2019; pp. 309–314.
102. Yeung, Y.; Lu, W.; Xue, Y.; Huang, J.; Shi, Y.Q. Secure binary image steganography with distortion measurement based on prediction. *IEEE Trans. Circuits Syst. Video Technol.* **2019**, *30*, 1423–1434. [CrossRef]
103. Arunkumar, S.; Subramaniyaswamy, V.; Vijayakumar, V.; Chilamkurti, N.; Logesh, R. SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images. *Measurement* **2019**, *139*, 426–437. [CrossRef]
104. Holub, V.; Fridrich, J. Digital image steganography using universal distortion. In Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security, Montpellier, France, 17–19 June 2013; pp. 59–68.
105. Amritha, P.; Sethumadhavan, M.; Krishnan, R.; Pal, S.K. Anti-forensic approach to remove stego content from images and videos. *J. Cyber Secur. Mobil.* **2019**, *8*, 295–320. [CrossRef]
106. Fridrich, J.; Goljan, M.; Du, R. Reliable detection of LSB steganography in color and grayscale images. In *Workshop on Multimedia and Security: New Challenges*; Association for Computing Machinery: New York, NY, USA, 2001; pp. 27–30.
107. Fridrich, J.; Kodovsky, J. Rich models for steganalysis of digital images. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 868–882. [CrossRef]
108. Dalal, M.; Juneja, M. Steganography and Steganalysis (in digital forensics): A Cybersecurity guide. *Multimed. Tools Appl.* **2021**, *80*, 5723–5771. [CrossRef]
109. Bagnall, R.J. Reversing the steganography myth in terrorist operations: The asymmetrical threat of simple intelligence dissemination techniques using common tools. *SANS Inf. Secur. Read. Room* **2002**, *19*. Available online: https://www.sans.org/reading-room/whitepapers/stenganography/paper/556 (accessed on 28 April 2021).
110. Mihalache, D. *Child pornography in Internet*; Analele Universităţii Libere Internaţionale din Moldova (Seria Economie): Chisinau, Moldova, 2009; pp. 225–229.
111. Mazurczyk, W.; Wendzel, S. Information hiding: Challenges for forensic experts. *Commun. ACM* **2017**, *61*, 86–94. [CrossRef]
112. Stier, C. Russian Spy Ring Hid Secret Messages on the Web. Available online: https://www.newscientist.com/article/dn19126-russian-spy-ring-hid-secret-messages-on-the-web/ (accessed on 28 April 2021).

113. Dhawan, S.; Gupta, R. Analysis of various data security techniques of steganography: A survey. *Inf. Secur. J.* **2021**, *30*, 63–87.
114. Taylor, M.; Haggerty, J.; Gresty, D.; Lamb, D. Forensic investigation of cloud computing systems. *Netw. Secur.* **2011**, *2011*, 4–10. [CrossRef]
115. O'shaughnessy, S.; Keane, A. Impact of cloud computing on digital forensic investigations. In *Ifip International Conference on Digital Forensics*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 291–303.
116. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; et al. A view of cloud computing. *Commun. ACM* **2010**, *53*, 50–58. [CrossRef]
117. Baldwin, J.; Alhawi, O.M.; Shaughnessy, S.; Akinbi, A.; Dehghantanha, A. Emerging from the cloud: A bibliometric analysis of cloud forensics studies. In *Cyber Threat Intelligence*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 311–331.
118. Topi, H.; Tucker, A. *Computing Handbook: Information Systems and Information Technology*; CRC Press: Boca Raton, FL, USA, 2014; Volume 2.
119. Zimmerman, S.; Glavach, D. Cyber forensics in the cloud. *IA Newsl.* **2011**, *14*, 4–7.
120. Freet, D.; Agrawal, R.; John, S.; Walker, J.J. Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS. In Proceedings of the 7th International Conference on Management of Computational and Collective Intelligence in Digital Ecosystems, Caraguatatuba, Brazil, 25–29 October 2015; pp. 148–155.
121. James, J.I.; Jang, Y. Practical and legal challenges of cloud investigations. *arXiv* **2015**, arXiv:1502.01133.
122. Choo, K.K.R. Legal issues in the cloud. *IEEE Cloud Comput.* **2014**, *1*, 94–96. [CrossRef]
123. Snaith, B.; Hardy, M.; Walker, A. Emergency ultrasound in the prehospital setting: The impact of environment on examination outcomes. *Emerg. Med. J.* **2011**, *28*, 1063–1065. [CrossRef] [PubMed]