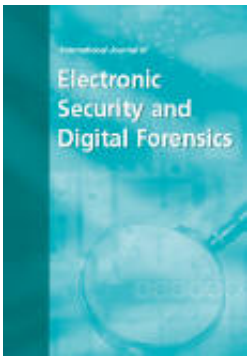

International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

Cloud forensics and digital ledger investigation: a new era of forensics investigation

Abdullah Ayub Khan, Aftab Ahmed Shaikh, Asif Ali Laghari, M. Malook Rind

DOI: 10.1504/IJESDF.2023.10045851

Article History:
Received: 09 November 2021
Accepted: 23 January 2022
Published online: 15 December 2022

Cloud forensics and digital ledger investigation: a new era of forensics investigation

Abdullah Ayub Khan*

Department of Computer Science,
Sindh Madressatul Islam University,
74000, Karachi, Sindh, Pakistan
and
Department of Computing Science and Information Technology,
Benazir Bhutto Shaheed University Lyari,
75660, Karachi, Sindh, Pakistan
Email: abdullah.khan00763@gmail.com
*Corresponding author

Aftab Ahmed Shaikh, Asif Ali Laghari and M. Malook Rind

Department of Computer Science,
Sindh Madressatul Islam University,
74000, Karachi, Sindh, Pakistan
Email: aftab.shaikh@smiu.edu.pk
Email: asif.laghari@smiu.edu.pk
Email: malook.rind@smiu.edu.pk

Abstract: Nowadays, cloud computing has gained popularity because it provides a platform for pay-as-you-go services, including hardware, software, and operating environment. However, technological resources cannot only be shared, but allocated on-demand to various users. With the emerged rate of inevitable vulnerabilities and network crime activities all over the globe, cybercriminals targets cloud environments. So, the demand for digital investigation is increased drastically. These extreme challenges pose serious issues for the cloud investigation. It has an impact on the researcher community of digital forensics as well. The cloud service providers and customers have yet to establish adequate forensics capacity and support digital forensics investigations on cybercrime activities in the cloud. In this paper, we present a digital forensics-enabled cloud investigation framework. In addition, we survey previous related works based on existing cloud forensics practices, fog forensics, edge forensics, and law and highlight the significant role of cloud computing in digital forensics. Finally, we discuss the technical challenges and limitations along with the future directions.

Keywords: cloud forensics; digital ledger investigation; cybercrime; cloud computing; edge computing; fog applications.

Reference to this paper should be made as follows: Khan, A.A., Shaikh, A.A., Laghari, A.A. and Rind, M.M. (2023) 'Cloud forensics and digital ledger investigation: a new era of forensics investigation', *Int. J. Electronic Security and Digital Forensics*, Vol. 15, No. 1, pp.1–23.

Biographical notes: Abdullah Ayub Khan is currently pursuing his PhD with the Department of Computer Science, Sindh Madressatul Islam University Karachi. He has published around 20 research articles in well-reputed journals (such as *IEEE Access*, MDPI, Elsevier, Spring and Wiley) in the domain of digital forensics, cyber security, blockchain, hyperledger technology and artificial intelligence.

Aftab Ahmed Shaikh has obtained his Doctorate in Computer Application and Technology from the Beijing University of Aeronautics and Astronautics (BUAA) in 2010. He has more than 18 years of professional experience in teaching and research in different countries including Pakistan, China and Oman. He is associated with a number of reputable research communities and editorial boards. He is a well-published author of several research articles in reputable international journals and conference proceedings. He has supervised several dissertations and projects and leading a research group of computational intelligence (CI).

Asif Ali Laghari obtained his PhD in Computer Science and Technology from the Harbin Institute of Technology (HIT), China, in 2019. He is the author of over 55 research articles in HEC recognised and impact factor journals, conferences, and two book chapters of international repute. His research interests include cloud computing, quality of experience, multimedia streaming, fog computing and social networking.

M. Malook Rind is a Professor of the Computer Science Department at Sindh Madressatul Islam University (SMIU), Karachi, Pakistan. He obtained his PhD in Information Technology (IT) from the International Islamic University Malaysia. He has more than 18 years of diversified industry, teaching and research experience. He is an author of one book and has over 40 published articles in various ISI, Scopus, IEEE, recognised journals and international conferences. His research interests include data communication networks, software-defined networking, electronic and mobile commerce, network security, pervasive computing, cloud computing, social networking and information systems.

1 Introduction

In the modern era of information technology, cloud computing is becoming one of the most transformative computing technologies, because of multimedia systems, such as mainframes, minicomputers, and desktop computers, mobile and ubiquitous devices. The World Wide Web and mobile applications are examples of such technology (Ruan et al., 2011). However, cloud computing entirely changes the lifecycle of information technology services that are created, accessed, managed, and delivered. For instance, the cloud services market is growing 17.5% in 2019 with a total of $214.3 billion up from $182.4 in 2018. These are the approximate 30% increase in numbers throughout the world public markets. The prediction of the worldwide public cloud services market will reach approx. $331.2 billion in 2022[1]. As cloud services are growing rapidly, in this regard, the size of the average cases of digital forensics is increasing by 15.9% during the forecast period between 2019–2020 (and the average prediction is $4.62 billion in 2017 to $9.68 billion in 2022)[2]. As a result, the ability to timely process massive forensics data

that can be processed is outgrowing, which demand the use of large-scale distributed resources to customise the processing (Roussev et al., 2009).

However, cloud technology has gained more popularity with various vulnerabilities and not aggravates the issues of scalability and flexibility for the activity of digital forensics but creates a unique platform to investigate cybercrime activities. Practitioners of cloud computing environment and digital forensics tools extend the expertise in cyber investigation. However, cloud forensics provides a new way of digital investigation, incident response, and evidence preservation. The application of digital forensics in a cloud environment consists of a hybrid forensics science approach, such as thin-client, thick-client, remote, virtual, etc., towards the age of digital evidence collection and examination (Ruan et al., 2013). Cloud forensics is a cross-discipline between digital forensics and cloud computing that mainly focuses on the collection of digital forensics information (evidence). For instance, the main concern for a digital investigator is to protect the digital evidence and chain of custody, which also ensuring that it could not be tamper or forge. To protect the evidence chain of custody from any third-party accessibility, the investigator creates a secure preservation and protects this evidence with the hash encrypted (SH-256) ledger, so this can securely be present in a court of law. In cloud computing, the customers depend on the cloud service providers (CSPs) for accessing the logs in the cloud. Sometimes CSPs hide the details of the logs according to the policy they offered. In this regard, maintaining the chain of custody in a cloud environment is becoming a challenging task. The security team (digital investigators) has no control to gather digital evidence over the policy of CSPs. That is a concerning the problem where the chain of custody may not hold in a court. These all could be because of a lack of training and protocols provided in accordance with the forensics standards (Dykstra and Sherman, 2011).

1.1 Cloud computing

The National Institute of Standard and Technology (NIST) defined cloud computing as "a model enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Khan et al., 2021a). In cloud forensics analysis, understand and study each aspect and its impact on the most essential characteristics of cloud computing. The characteristics of cloud computing are on-demand self-service, resource pooling, rapid expansion, access to a broad network, and managed services (Laghari et al., 2016). There is a list of three service models such as software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) (Laghari et al., 2017). Furthermore, the four main deployment models are public, private, hybrid, and community, which provide ways to deliver cloud services (Kumar et al., 2019).

In cloud computing, forensics-as-a-Service (FaaS) offers integrated end-to-end forensics services over the cloud (Srinivasan and Ferrese, 2019). A CSP provides on-demand forensics services and facilities to experts for digital investigations, such as gathering electronic evidence and ensuring the integrity of the information. In late 2010, the Forensics Institute of Netherlands proposed a service-based scheme [called digital forensics as a service (DFaaS)] for digital investigation of high volume seized information and overall investigational processes (Sarkar and Das, 2014). After the

experience, several cases and many investigators shifted and rely on the standard of this scheme, not only utilised in the Netherlands abroad, but also used according to the court of law (Bhoedjang et al., 2012). In 2015, van Beek et al. presented the high impact on forensics data when analysing big data, explore design principles (for example, privacy, security, and transparency), and implement centralised DF services. After a couple of years, Raju et al. (2016) proposed forensics enabling as a service framework for digital investigators to investigate incidents, malicious attacks, and analysis of the lack of security inside and outside of virtual machines (VMs) over the cloud environment.

1.2 Digital forensics

Digital forensics (DF) refers to "the application of forensics science to identify an incident by collection, examination, and analysis of digital data while preserving the integrity of the evidence" (Kent et al., 2006b). For efficient utilisation of time and resources, and capability of the digital forensics investigation process to extract potential evidence from the collected evidence in a crime scene is the biggest requirement (Chang et al., 2019). The process of digital forensics is categorised into six crucial phases (Selamat et al., 2008):

1 *Identification:* Two steps involved such as identifying the purpose of investigation and the required resources.

2 *Preservation:* Ensure data is isolated and secure means overall data integrity.

3 *Collection:* A step in which the evidence is acquired, seizing physical assists such as mobile devices, personal computers, etc., make sure maintaining the integrity of the collected data, keep the media storage original in a pristine state.

4 *Examination:* The phase is divided into three main parts, preparation, extraction, and identification; the main purpose of this phase is to study the attributes of the collected data.

5 *Analysis:* Examiners identify data, process, utilisation of related tools and techniques, and interpret results analysis.

6 *Presentation:* With the help of gathering facts, a report presents in a court of law that concludes the summarised process and explanation of the related case.

Digital forensics is the science of finding digital evidence from digital technologies such as mobile phones, personal computers, damaged hard drives, SD cards, servers, and so on. The main objectives of the digital forensics team are to identify digital evidence, inspect, analyse, and preserve data on various types of electronic devices, and their crucial importance are as under:

- the main aspect of digital forensic is to recover material in such a manner that helps in the evidence chain of custody
- postulate the main motive behind the crime
- identify the main culprit
- identify evidence very quickly
- estimate the potential impact of malicious activities
- producing a complete investigational process report.

1.3 Cloud forensics

NIST defines cloud computing forensics science as "the application of scientific principles, technological practices, derived, and proven methods to reconstruct past cloud events through the process of forensics science such as identification, preservation, collection, examination, analysis, and presentation of digital evidence" (NIST Cloud Computing Forensic Science Working Group, 2018). Pichan et al. (2015) have defined cloud forensics as "the application of digital forensics in the cloud computing environment. A subset of network forensics is considered as a cross-discipline area". The default nature of the technology adds multilayers of complexity in cloud forensics, such as a high degree of virtualisation, data duplication, jurisdiction, and multitenancy. Therefore, Alex and Kishore (2017) highlight three critical cloud forensics significant issues such as organisational, technical, and legal. The interaction between cloud actors for digital forensics investigation incorporates organisational aspects of cloud forensics. Technical aspects deal with forensics tools and techniques, which means the overall procedure and mechanisms. Finally, legal aspects are something that used to manage multijurisdictional and multitenant situations.

Despite the significant aspect of cloud forensics investigation is discussed, there are several new ways that drive to investigate forensics process and cloud-based crimes and discuss the applicability of forensics science to a cloud environment and their impact. In this scenario, we reviewed some cloud forensics literature, where the researchers' main concerns on cloud security issues and challenges, such as the lack of secure investigational models and frameworks. Whereas the collaboration of cloud services for forensics science emerges many aspects, especially from a security perspective, the difference between the traditional and current process of investigation a framework for cloud forensics investigation. Unfortunately, the proposed architectures of cloud computing do not design that help in real-time process of forensics investigation and create chain of custody security, still the architecture are not feasible to seize files from data servers without violating the privacy of other users (Zawoad and Hasan, 2013). Simou et al. (2014a) categorise the list of cloud forensics challenges in which the identification stage [for example, physical inaccessibility, volatile data distribution, client-side identification, trust dependency, and service level agreement (SLA)], preservation (with integrity and stability, privacy, time synchronisation, internal staffing, chain of custody, multi-jurisdiction, and multi-tenancy), examination and analysis (lack of forensics tools, the volume of data, encryption, reconstruction, identity, and log format), presentation (complexity of testimony, and documentation), and compliance issue discuss in brief.

A recent survey reported the challenges of cloud forensics and addressed by both parties such as researchers' community, and government agencies. However, many challenges remain untouched to be resolved (said by Manral et al., 2019) yet. Utilisation of large-scale internet around the world that might be exposed to cyberthreats is highly on the cloud server, and it is very challenging to apply the forensics approach specifically in conducting cloud investigations. Unfortunately, the rate of cyber threats increases in the past few years; behind this, there is a lack of sufficient digital investigation. Consequently, cloud investigation needs to recognise any crime incidents that happened in cloud computing services. Yassin et al. (2020) discussed the cloud forensics challenges according to the phases of digital investigation along with a recommendation. This paper includes the physical location, SLA issue, system-level logs, data issue, decentralised

logs, lack of trust, logging, and others. In this paper, Section 6 provides a detailed description from a solution point of view of the current challenges, issues, and limitations that emerged in the technology.

The characteristics of cloud computing and features in digital forensics environment are listed as:

1 volatility

2 virtualisation

3 elasticity

4 multi-tenancy

5 multijurisdictional.

According to the criminal incident that occurs in a cloud environment, the design and implementation of digital forensics process models for digital investigation changed, for example, client-side forensics, server-side forensics, and consumer-oriented forensics (Reddy, 2019). A customer-oriented cloud forensics process model (Moussa et al., 2019) is one of the most useful process models in real-time. This aimed cloud consuming organisations start with cloud forensics readiness method. Whereas local analysis is required when transferring forensics data from cloud servers to the premises of a consumer organisation, after that, the steps of digital forensics (legal and contractual review, documentation, and preservation) are investigated by the process model (Moussa et al., 2019). Cloud is used by consumers to access cloud services, whereas malicious attackers target cloud consumers to exploit the vulnerabilities of cloud services. Khan et al. (2021e) proposed a method that supports the design and implementation of cloud services to make cloud forensics enabling services. Zawoad et al. (2013) introduced secure logging as a service that stores a virtual log and provides access to the digital investigator to ensure users' integrity and confidentiality. Undoubtedly, the contributions in the field of cloud forensics fulfil the gaps, but most of the sections remain untouchable, which need more consideration to overcome the technical issues and limitations.

1.4 Impact of edge computing in digital forensics

The majority of these day's criminal activities are direct conduct at the edge of the network (Razaque et al., 2021). The development and popularisation widespread between network and computer technology, which have changed the way of traditional production, management, and life, and also provide new opportunities and development for cybercriminals to flourish (Razaque et al., 2021; Prakash et al., 2021). The activities of cybercriminals have increased and computer-based knowledge driven investigations and many computer crimes have become commonplace (Shalaginov et al., 2020). For instance, theft, destruction of information privacy, and integrity, attacks, fraud on government level, pornographic information, server-based applications, and web flooding (Deebak et al., 2020). Detection of such cases requires edge computing and network forensics to search for and trace and confirm the identity of the cybercriminals and the evidence chain of custody, and in accordance to bring charges against the accuse (Prakash et al., 2021; Math et al., 2021).

1.5 Fog forensics investigation and security features

Fog computing is a decentralised infrastructure located on IoT-multimedia devices for enable storage and communication and the overall management of IoT-based forensics investigations (Alzoubi et al., 2021). Fog computing intermediates cloud-forensics framework and extends the services of cloud investigation (Mukherjee et al., 2020). However, it does not mean that this technology replaced cloud computing. It provides on-demand forensics investigation applications and services to cloud-based multimedia devices (Hegarty and Taylor, 2021). For instance, the fog node helps resource constraint multimedia devices to conduct computational processes that consume more power and resources (Alzoubi et al., 2021; Almaiah and Almomani, 2020). In addition, it enables multimedia devices to meet the requirements of delay sensitivity for certain applications, which overcome the limitation of network bandwidth (Almaiah and Almomani, 2020). As an extension to the cloud environment, fog inherits some challenges from cloud-forensics, especially chain of custody, security and privacy and secure preservation limitations (Alzoubi et al., 2021; Arpit and Mandhar, 2021). Due to the lack of security and resource constraint nature, multimedia devices are easy to compromise (Arpit and Mandhar, 2021). To protect devices and collect evidence, the fog environment does not have any sophisticated tools and techniques to prevent forensics chain of custody. This is due to the unique features of fog decentralised infrastructure, or may be a different providers of fog nodes, and the resource-constraint nature of nodes (Xu et al., 2020; Rani et al., 2021).

This paper addresses the topic of cloud forensics and the nature of cloud crime and compared with other state-of-the-art cloud research orientations, trends, and technical issues of cloud forensics; and so, how cloud forensics is used in the process of digital investigations. For the detection of a network, host, and live edge computing-based digital investigation is also discussed which is one of the challenges issues raising nowadays. Moreover, it surveys the various frameworks of cloud forensics and processing layers of forensics science that help to collect digital crime incidents and attacks on cloud investigations, such as identification, collection, examination, analysis of digital data, and preserving information integrity. In this paper, we also highlight some technical issues and limitations in the previous work and discuss future work challenges and development. Furthermore, we have analysed and addressed a set of open research areas yet to be discussed in the domain of cloud forensics.

The rest of the paper is organised as follows. Several relevant cloud forensics frameworks are highlighted in Section 2. The relationship between forensics science and cloud is discussed in Section 3. The readiness for digital forensics on the cloud environment is depicted in Section 4. The limitations of the current technology and the solution proposed for mitigating those challenges are discussed in Section 5. In Section 6, we mention open areas of cloud forensics for continued research. Finally, we concluded the research in Section 7.

2 Cloud forensics frameworks

In the cloud forensics environment, we frame the approach of digital forensics investigation that helps in the overall procedure and guides the forensics activities. Since 1995 more than fourteen frameworks proposed by different forensics experts, plentiful

digital forensics investigation frameworks often choose a combination of approaches, developing processes according to particular personnel, budget, and workload (Selamat et al., 2008). Generally, framework-to-framework variation occurs in the processes of model design because of the cloud incidents, mostly the simple process of cloud forensics is a collection, examination, analysis, and reporting. Whereas collection is the process used to acquire physical data, combing of data items occurs in the examination process. In the stage of forensics analysis, the digital forensics examiner examines individual evidence at the crime scene and reports and presents these documents in a court of law.

In 1999, McKemmish defined the first successful forensics framework as shown in Table 1. Kent et al. (2006a) presented the NIST framework in 2006. Similarly, Martini and Choo (2012) proposed a framework with some positive variation in the steps of digital forensics. Finally, Alex and Kishore (2017) present a cloud forensics framework according to state-of-the-art shown in Table 1.

Table 1 Cloud forensics framework comparison (phase-to-phase)

McKemmish (1999)	*NIST framework (Kent et al., 2006a)*	*Martini and Choo (2012)*	*Alex and Kishore (2017)*
Identification	Collection	Identification and preservation	Identification depends on cloud service provider and preservation
Preservation	Examination	Collection	Collection
Analysis	Analysis	Examination and analysis	Monitor and analysis
Presentation	Reporting	Reporting and presentation	Reporting and presentation

Nowadays, the internet of things (IoT) is gaining increasing attention; a great number of research has focused on this field, and research on digital forensics investigation is moving a little focused towards IoT (Islam et al., 2019). The existing platform of IoT has not mature enough to fully adopt the current methods, tools, techniques, and procedures of digital forensics. For the IoT infrastructure, a generic digital forensics investigation framework was proposed by Kebande and Ray (2016). Apart from this, Li et al. (2019) proposed a novel blockchain-based digital forensics investigation framework that collaborates with IoT and social systems environments. Across jurisdictional borders, the decentralised nature of blockchain technology helps to preserve the integrity and origin of collecting evidence for digital investigation. A recent survey reported (Stoyanova et al., 2020; Yaqoob et al., 2019) related to the challenges, issues, limitations, approaches, open areas, readiness, and the relationship between IoT and forensics science, which discuss in the next couple of sections.

3 Relationship between digital forensics and cloud computing

Traditional digital forensics involves seizing devices and suspected user storage media, which allow investigators to acquire, preserve, analyse, and present digital evidence in front of the court of law. The collaborative environment and the rapid increment in the size of cloud media storage create significant issues for traditional approaches, tools, and techniques. To prove the incident occurred and the evidence is permissible in a judiciary, the high demands for the arrangement of sufficient and clear evidence. Categories of

potential digital forensics artefacts according to incident physical and logical locations are:

1 network

2 client

3 cloud service provider.

The network location can handle the access logs, transaction logs, header, and package content. On the other side, chat logs, firewall logs, access logs, browser logs, web content, application cache, and host intrusion detection are possible sources of evidence gathered through client locations. Cloud service provider location helps to collect firewall logs, admin access logs, IDS, data storage, and NetFlow data artefacts. Moreover, there is a distinct nature of cloud crime and the way to perform an investigation to gather the possible source of evidence that can significantly assist digital forensics experts.

3.1 Nature of crime

Digital crime is sometimes known as computer-related crime (Taylor et al., 2014), a crime attempted by using cloud services, either as a tool or subject, and an object considering the nature of cloud computing crimes (Taylor et al., 2011; Chen, 2014). In the objective of cloud computing crime, cloud service provider has been the target, such as denial of service (DoS), distributed denial of service (DDoS). When the cloud platform is used to conduct crime, consider the subject nature of cloud crime. To identity theft is one of the biggest examples in the recent era. There is another nature of cloud computing crime based on computer tools, a cloud service attack to other cloud service networks such as dark clouds (Fu et al., 2010).

3.2 Performing investigations

The current digital cloud forensics investigation is split into two sub portions, namely: performing the investigation in and on the cloud environment. Performing an investigation is a case based on evidence located in the cloud. A cloud service provider must be aware of the incident response strategy, such as identification, notification, and recovery, and the organisation of digital forensics methodologies. Unlike investigation in the cloud, cloud computing provides on-demand services of network forensics that have more computational power, storage and speed up the investigation analysis capability in distinct areas, for example, sorting, hashing, and searching evidence (Corey et al., 2002; Khan et al., 2014). Recently, forensics-as-a-service (van Baar et al., 2014) is a remote interface that used to access and analyse suspected data, provides datacentre capability for digital forensics investigators to store digital evidence like image seizing devices, outsource storage.

In digital forensics, snapshots are significant for security research, as it is the state of a system at a particular point in time, a logical copy of the volume content that consumes minimal storage space (Huber et al., 2011). Snapshots are considered as a source of evidence for services provided either through distributed systems or virtualisation environments. As the current approaches give the reliability of taking snaps, the forensics purpose needs investigation. However, the proactive measure of cloud users checks the

availability of offline virtual environment snapshots, for example, Amazon Elastic Computer Cloud (EC2) along with the Amazon Elastic Block Storage (EBS) provides storage services (snapshots of the users' storage) (Martini and Choo, 2014). In the situation of digital attacks, snapshots can be analysed offline without tampering the original storage and tackle the disturbance of a business operation.

4 Cloud computing readiness for digital forensics

Cloud computing is the current technology trend, distinct standardised bodies have initiated a cloud forensics framework to cope with the rapid adaptation of cloud services (Almulla et al., 2014), like SaaS, PaaS, IaaS and the most prominent implementation is FaaS that mentioned in the above section. Initially, enhancing the existing security of cloud computing and digital forensics guidelines, assessing involving an itemised list of data and applications that move to the cloud with minimal impact on the business operations, for example, transition proceeds. The primary goal of cloud readiness is to provide a gap analysis of organisations and make a list of prescriptive cloud applications that move smoothly (Loebbecke et al., 2012). In this paper, we discuss, the two most crucial cloud computing readiness for digital forensics are as under:

4.1 Distributed computing

D. Peleg defined distributed computing (DC) as "a model in which multiple computer systems are working on a single problem" (Roussev and Richard, 2004), also described as "components of a software system are shared by multiple computer systems to improve performance in terms of efficiency and accuracy". The main objective of DC is to maximise the performance due to this, connecting IT resources and users in a transparent, reliable, and cost-effective manner.

4.1.1 Distributed computing forensics tools

Traditionally, investigative tools execute on a single workstation, each has reached a clear limit, and inhibit timely processing evidence (Roussev and Richard, 2004) that considers a giant challenge in digital investigation environments. Cohen et al. (2011) proposed a rapid response framework, an open-source multiplatform distributed digital forensics investigation tool that enables remote access of memory and raw disk storage. The primary processes of distributed forensics investigation are as follows:

- create an image of the user storage
- calculate the hash values of the image storage files
- compare the generated hash values
- target files in the memory remotely according to the hash values.

In a cloud environment, continuous observation of network traffic and ensure the validity, a distributed relevant problem of a network forensics investigation that needs consideration. In this scenario, Spiekermann et al. (2017) proposed an open-source distributed tool based on an agent to perform digital forensics investigations in the cloud

environment. The DC environment is used to conduct an incident to examine the feasibility of the DF acquisition tool. The process to gather deleted files and undeleted files from workstations either reside internally or externally the investigators' jurisdiction.

4.1.2 Distributed computing impact on digital investigation

In cloud forensics investigation, a distributed file system (DFS) is a cloud storage technology that manages the entire files and metadata of cloud users. Google file systems (GFS) is designed and implemented as a scalable distributed file system for substantial data-intensive distributed applications; it provides inexpensive commodity hardware, fault tolerance, and high aggregated performance (Ghemawat et al., 2003). Hadoop (HDFS) is an open-source platform that provides large clusters to store datasets on thousands of servers that host directly the execution of user applications (Shvachko et al., 2010; Spiekermann et al., 2017; Soltys, 2020), more reliable, and requires high bandwidth to stream users' application datasets. HDFS is widely used as a distributed filesystem where the architecture is slightly different from the GFS. Let us consider an incident, software bug displaying private messages of users on their public profiles; this is because of an internal architecture failure that violates users' privacy. Understanding the architecture of these two DFS is not probably the system aiding diagnosis but the need to learn in DF investigation.

The distributed architecture consists of groups of clusters, where each has master and chunk servers. Chunk servers contain files or content transition information, while the master server contains metadata, user logs, and connection logs, and non-constant information. In a digital investigation, the digital examiner rebuilds files from the file system either the content information located in chunk servers and non-content from the master server. In GFS (Ghemawat et al., 2003), user files are split into two portions, the 64 MB size of a chunk can store user files on the chunk server, and the master server maintains metadata, namespace, control, access, current location, and mapping information. For making the availability of servers, the master creates a duplication shadow server of DFS.

4.2 Virtualisation

A method of combining the resources available through the network, separate and distinguish the resources, and divide up the available bandwidth into distinct channels. The cloud service provider (CSP) offers cloud-based infrastructure or storage availability, software services, and platform on-demand scalable pay-as-you-go utilisation of cloud services. Amazon is the most popular CSP based on virtualisation technology. Since 1980 till present, cyber hackers are arrested for performing malicious attacks such as DoS, DDoS, and many others; attacks on Amazon EC2, eBay, Microsoft, Facebook, etc. (Middleton, 2017). It had a significant impact on cloud users not to conduct business services, online business transactions, depending on the web services interface hosted cloud infrastructure.

Amazon Web Services (AWS) is a broadly adopted cloud platform, offering services from the data centre globally. The DDoS attack on cybersecurity core curriculum objectives, that is, AWS information availability, computer system, and communication

channel functioning concurrently and correctly. AWS mitigate DDoS by utilising three customer tools at their disposal (Soltys, 2020):

- Router 53
- Cloud Front
- Shield.

There are all three customer-based tools which work together with edge location, location utilises giant cache, accelerates AWS actual caching applications (Soltys, 2020).

4.2.1 Virtualisation forensics tools

In a virtual environment, several cloud virtualisation tools develop that monitor hypervisors or virtual machines for digital forensics investigation, identify and retrieve evidence from a virtual machine (VM) instance that configures with persistent storage. Virtualisation tools used in cloud computing forensics for load balancing, aggregation of available resources, and automatic monitoring of malicious attacks (Masood et al., 2014). Virtual introspection is a built-in method to monitor virtual instant states; this tool can help for network or live forensics examiners to extract evidence from a virtual machine monitor (VMM) in the cloud environment.

4.2.2 Impact of virtualisation on digital investigation

In the context of DF, the forensics investigation on the cloud virtualisation either as computing, and hardware, software resources, distinctness is generated based on the particular location and functionality of a hypervisor. Cloud hypervisor enables the abstraction layer between cloud users' hardware and virtual machine instances. The virtualisation layer handles the host storage and server virtualisation as well as maintains the level of control of cloud users and service providers in the cloud environment. CSP controls virtual machine instances that provide to the users independently available virtual services through the cloud model of virtualisation. Rapid growth and high demand for cloud resources and virtualise storage led to the development of cloud forensics. To monitor individual VM, malicious attacks, threats, and illicit activities that can harm other systems and hide the actual identity in the virtual environment. Cloud forensics enables to manage these kinds of virtualisation challenges and limitations.

Hence, the cloud computing readiness for digital forensics can be achieved by intensifying the latest distributed computing and virtualisation technology, focusing on the heterogeneity of cloud research and the need to develop scientific methodologies for cloud forensics future readiness design that aid in the development.

5 Cloud forensics technical challenges, issues and limitations

As cloud computing is getting more popular in the past decade, and the advent of digital forensics makes technology towards the next level, the collaboration of cloud and DF creates a new area called cloud forensics that becomes a hot topic for digital forensics researchers. Cloud forensics is an emerging technology, most of the portions successfully implemented that robust the system capabilities, for example, FaaS, but on the other side,

the technologies need concentration on technical challenges, limitations, and issue rises in the past few years. The challenges are as follows:

5.1 Forensics data acquisition

Digital forensics data acquisition targets on single computer systems and isolated environment, on the other side, the cloud data acquisition processes contain complex infrastructure, such as distributed and virtualised environments, for example, application software, virtual network, and storage, with distinct platform availabilities (Barrett, 2020). The current forensics acquisition process maintains a chain of custody and control state of unaltered digital evidence. However, cloud forensics data acquisition is not feasible due to the complexity of cloud computing, requiring the development of newly acquired methods, and educating technical managers accordingly the technological changes in the complete process of cloud forensics acquisition.

5.2 Chain of custody

The most critical process starts with the collection of computer-assisted evidence (Chopade et al., 2019), significant for digital investigation, especially, preserve the history of the documentation, and provide details about the evidence collection, examination, analysation and seize in the storage in order to present in the court of law. In digital forensics, the chain of custody works on a simple mechanism, that is, forensics investigators preserve information and deliver the evidence reported to the judiciary of law. However, in the cloud, the nature of distributed crime changes the overall mechanism; collect data from a remote server, seize in the secure channel of storage media, validate evidence, and make a copy of the information available during the time for the cloud forensics investigators.

5.3 Limitations of current forensics tool

Various digital forensics tools are available to collect data from the crime scene, identify, examine, analyse, validate, preserve, and make a proper report. Automate the analysis of cloud crime is an emerging problem; OpenNebula and NetworkMiner is an example of network forensics tools that capture data packages and analysis the collected records of the virtual environment. Unfortunately, there are no specific cloud-based automatic incident analysis tools. Cloud investigators use DF as existing tools for acquiring digital evidence, requiring a new development of cloud-based stimulated forensics tools that perform live investigations without the intervention of human agents.

5.4 Evidence segregation

Several virtual machine instances running on the same IT-based infrastructure, controlling each VMs by a virtual machine monitor (VMM), are isolated as well as create an individual via a hypervisor. Undoubtedly, this scenario considers the essential characteristics of cloud computing that reduces IT costs and increases resource pooling. However, this is one of the critical issues for cloud forensics to segregate digital evidence from each VM instance, treated on a single host, with no access to each other despite it

hosted on the same IT infrastructure. For the investigation, evidence segregation of individual instances is crucial, as well as CSP ensuring the evidence integrity and confidentiality over the cloud environment.

5.5 Internal staffing and external dependency

Nowadays, cloud forensics experts utilise digital forensics and network forensics procedures and tools, which is a critical exercise to acquire, retrieve, examine, and analyse cloud incidents. A major technical challenge in cloud forensics investigations is internal staffing (Simou et al., 2014b); the need to have trained staff according to forensics research law and regulations, and rapidly evolving cloud technologies and tackle the entire internal technical and legal challenges. On the other side, cloud service providers and other cloud applications depend on the third-party cloud service providers leading to the external dependency. The problem arises when an interruption occurs and lacks coordination between parties, the reason behind why virtual forensics investigations non-existent.

5.6 Cross-border law

It is hard to investigate cross-border incidents (Zargari and Benford, 2012), especially data protection activities, and follows the laws and regulations of information technology on a governmental level. Analysis of cloud-based threats and privacy according to the legal procedure of country law, this becomes a challenging aspect in the domain of cloud forensics. The cross-border investigation access to the resource pooling of IT infrastructure over the cloud may require a new path to identify the solution rather than to the traditional process of DF, for example, collection, examination, analysation, preservation, documentation, and presentation defined by NIST in 2006.

5.7 Service level agreement

As cloud computing provides cloud services on-demand, there is a documented contract signed between the cloud client and CSP which defines the terms and conditions of usage of virtual resources. The purpose highlights the service level agreement (SLA) issue because there are no provisions for digital investigation as well as the recovery of evidence (Khan et al., 2021b). The clause should incorporate in the agreement, moreover, mention the legal cloud, forensics regulations, evidence integrity, and document confidentiality before signing the SLA.

5.8 Multi-jurisdictions and tenant

In a virtual environment, the storage of data occurs distributed over various virtual locations; this scenario creates fault tolerance and more efficient to access it. Data distribution has become a challenging problem in terms of legal proceedings of multijurisdictional. Law enforcement agencies and the court of law can only take the subject matter of action when a matter has authorised jurisdiction over the parties.

The multitenant environment (Zawoad et al., 2015) is another challenging aspect of cloud forensics, the cloud service provider allows the cloud clients to avail services like infrastructure, share physical, server, hardware, and software concurrently. In this case, multiple users can share the same physical server storage as well as the network, virtually, a challenge to investigate the services used by an individual client, and switch to VMs can also create an impact on cloud investigation. However, CPS is unwilling to allow digital forensics investigators to access shared storage because it is totally against other cloud users' privacy policies.

Table 2 Open research areas of cloud forensics

Reference	*Proposed work*	*Challenges and limitations*	*Open research areas*
Grajeda et al. (2017) and Teing et al. (2017)	Digital forensics experts perform cloud investigations by using network and digital forensics tools and analyse virtual incidents over the cloud. However, the changes required in the existing DF method of manual collection of evidence artefacts ensure the reduction of data correlation and the need to conduct automatic or manual intensive cloud investigations.	There are no proper cloud-specific forensics data acquisition tools available. A former gap between testing tools and cloud investigation datasets. An improper collection and selection of datasets make a considerable impact on testing.	Cloud forensics data acquisition tool testing
Baig et al. (2017) and Case and Richard (2017)	The lack of security and protection creates a negative impact on the cloud service and forensics artefacts. For example, before investigating and processing cloud client stored data, CSP may provide a complete description of the environment where the data collected information about the internal environment is valuable for investigation.	An internal infrastructure transparency poses a critical problem in cloud forensics investigations. Low transparency. High redundancy.	Cloud services and data transparency

Table 2 Open research areas of cloud forensics (continued)

Reference	*Proposed work*	*Challenges and limitations*	*Open research areas*
Peng et al. (2020), Pichan et al. (2018), Hosseinian (2015) and Battistoni et al. (2016)	In a generic cloud forensics framework, this may describe a concept of a forensics model that provides investigational services over the cloud. A generic model could implement the forensics services by considering the technical challenges of cloud forensics and change the existing cloud computing infrastructure along with assuring cloud forensics users that investigators could conduct high-quality investigations.	Data acquiring, collect, and preserve, as it controls the overall cloud infrastructure. Data package capturing and logging mechanism along with billing records.	Generic Framework
Nanda and Hansen (2016) and Masmoudi et al. (2017)	In cloud forensics, multitenant architecture configuration is the focus area of DF researchers nowadays; the implementation poses a challenging aspect, that is handling cloud big data, distributed systems, multijurisdictional, and lack of forensics services.	Multi-tenant architecture takes more time to implement. Lack of architecture support of forensics analysis. Lack of tools and investigational methods availability.	Cloud-based forensics configuration and multi-tenant architecture
Srivastava and Choudhary (2020), Fernandes et al. (2020) and De et al. (2020)	Cloud-enabled evidence capturing from multimedia-based portable devices and preserving the evidence in the protected storage is the process of the chain of custody. When a device requests to transmit digital information via intermediary storage, there is a signature between the client device and CSP, and the information is stored in the centralised file storage.	Digitally sign evidence metadata. Centralised file storage system. There is no digital signature between stakeholders. Less protected.	Blockchain enabled cloud evidence chain of custody

6 Open research areas

In this context, we have demonstrated the open areas that need a significant amount of attention and follow the state-of-the-art direction for the successful future of cloud forensics. Eventually, various technical limitations and challenges remain unsolved pertaining to the investigation, which need sophisticated solutions to enhance cloud

forensics investigation. We have highlighted the crucial open research areas of cloud forensics are as shown in Table 2.

7 Conclusions

This paper discusses the significant challenges and limitations in the current cloud forensics investigations and explains the need for cloud forensics in everyday life to secure information. Includes the evidence preservation and documentation of incident response and analysis. In fact, the technological main consideration prospects are to investigate the network crime and the cloud environment with latest mechanism of artificial intelligence analysis. However, the possibility of digital forensics investigation and cloud-related issues occurs in a real-world perspective, for example, multimedia streaming, and so on. In this regard, we have proposed a framework for secure forensics process-enabled cloud investigation system.

Moreover, the rapid growth of cloud users, because of virtualisation, elasticity, and flexibility of cloud computing make systems more attractive and reliable, but on the other side, there are several drawbacks, for example, authentication-related issues, privacy protection of ledger, and the scope of data. In fact, the low cost of cloud services pushes users to adopt cloud services. According to the security incident handling policies and framework, rises the need for forensically-based cloud services. In this paper, we differentiate the critical concepts of modern forensics science and digital forensics. Drive a new way to investigate cloud computing and its domains.

In this paper, we have discussed the concept of digital forensics and their escalation across various subparts, for example, network, live and mobile investigations, cloud forensics, and many others. However, the primary concern on the detection, identification, and behaviour analysis of cloud crime. Undoubtedly, it helps in the examination of cloud-related digital incidents and responses. It proposed distinct frameworks for cloud investigation in accordance with the domains. Moreover, we have discussed the appropriate relationship between cloud computing and forensics science to analyse the nature of attacks and coordinates to stop the misuse of a cloud environment. Also, we evaluate the current limitations, challenges, and technical issues in the cloud forensics investigation, the state-of-the-art cloud forensics research orientations, open research areas, and the future direction of cloud forensics.

References

Alex, M.E. and Kishore, R. (2017) ‘Forensics framework for cloud computing’, *Computers & Electrical Engineering*, Vol. 60, pp.193–205.

Almaiah, A. and Almomani, O. (2020) ‘An investigation of digital forensics for Shamoon attack behaviour in FOG computing and threat intelligence for incident response’, *Journal of Theoretical and Applied Information Technology*, Vol. 98, No. 7.

Almulla, S., Iraqi, Y. and Jones, A. (2014) ‘A state-of-the-art review of cloud forensics’, *Journal of Digital Forensics, Security and Law*, Vol. 9, No. 4, p.2.

Alzoubi, Y.I., Osmanaj, V.H., Jaradat, A. and Al-Ahmad, A. (2021) ‘Fog computing security and privacy for the internet of thing applications: state-of-the-art’, *Security and Privacy*, Vol. 4, No. 2, p.e145.

Arpit, B. and Mandhar, D. (2021) *A Survey on Enhancing Cloud Security Using Fog Computing*.

Ashraf, S., Kehkashan, T., Gull, M. and Moin u Din, S. (2018) 'Transparency service model for data security in cloud computing', *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, IEEE, pp.1–6.

Baig, Z.A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M. et al. (2017) 'Future challenges for smart cities: cyber-security and digital forensics', *Digital Investigation*, Vol. 22, pp.3–13.

Barrett, D. (2020) 'Cloud based evidence acquisitions in digital forensic education', *Information Systems Education Journal*, Vol. 18, No. 6, pp.46–56.

Battistoni, R., Di Pietro, R. and Lombardi, F. (2016) 'CURE – towards enforcing a reliable timeline for cloud forensics: model, architecture, and experiments', *Computer Communications*, Vol. 91, pp.29–43.

Bhoedjang, R.A.F., van Ballegooij, A.R., van Beek, H.M.A., van Schie, J.C., Dillema, F.W., van Baar, R.B., Ouwendijk, F.A. and Streppel, M. (2012) 'Engineering an online computer forensic service', *Digital Investigation*, Vol. 9, No. 2, pp.96–108.

Case, A. and Richard III, G.G. (2017) 'Memory forensics: the path forward', *Digital Investigation*, Vol. 20, pp.23–33.

Chang, D., Ghosh, M., Sanadhya, S.K., Singh, M., and White, D.R. (2019) 'FbHash: a new similarity hashing scheme for digital forensics', *Digital Investigation*, Vol. 29, pp.S113–S123.

Chen, H-Y. (2014) 'Cloud crime to traditional digital forensic legal and technical challenges and countermeasures', *2014 IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA)*, IEEE, pp.990–994.

Chopade, M., Khan, S., Shaikh, U. and Pawar, R. (2019) 'Digital forensics: maintaining chain of custody using blockchain', *2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, IEEE, pp.744–747.

Cohen, M.I., Bilby, D. and Caronni, G. (2011) 'Distributed forensics and incident response in the enterprise', *Digital Investigation*, Vol. 8, pp.S101–S110.

Corey, V., Peterman, C., Shearin, S., Greenberg, M.S. and Van Bokkelen, J. (2002) 'Network forensics analysis', *IEEE Internet Computing*, Vol. 6, No. 6, pp.60–66.

De, S., Barik, M.S. and Banerjee, I. (2020) 'A digital forensic process model for cloud computing', *2020 IEEE Calcutta Conference (CALCON)*, IEEE, pp.106–110.

Deebak, B.D., Al-Turjman, F. and Mostarda, L. (2020) 'Seamless secure anonymous authentication for cloud-based mobile edge computing', *Computers & Electrical Engineering*, Vol. 87, p.106782.

Dykstra, J. and Sherman, A.T. (2011) *Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies*, UMBC Computer Science and Electrical Engineering Department.

Dykstra, J. and Sherman, A.T. (2012) 'Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques', *Digital Investigation*, Vol. 9, pp.S90–S98.

Fernandes, R., Colaco, R.M., Shetty, S. and Moorthy, R. (2020) 'A new era of digital forensics in the form of cloud forensics: a review', *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, IEEE, pp.422–427.

Fu, X., Ling, Z., Yu, W. and Luo, J. (2010) 'Cyber crime scene investigations (C^2SI) through cloud computing', *2010 IEEE 30th International Conference on Distributed Computing Systems Workshops*, IEEE, pp.26–31.

Ghemawat, S., Gobioff, H. and Leung, S-T. (2003) 'The Google file system', *Proceedings of the nineteenth ACM Symposium on Operating Systems Principles*, pp.29–43.

Grajeda, C., Breitinger, F. and Baggili, I. (2017) 'Availability of datasets for digital forensics – and what is missing', *Digital Investigation*, Vol. 22, pp.S94–S105.

Hegarty, R. and Taylor, M. (2021) 'Digital evidence in fog computing systems', *Computer Law & Security Review*, Vol. 41, p.105576.

Hosseinian, A. (2015) 'Challenges of cloud forensics', *Enterprise Security: Second International Workshop, ES 2015*, 30 November to 3 December, Vancouver, BC, Canada, Revised Selected Papers, Vol. 10131, p.1, Springer.

Huber, M., Mulazzani, M., Leithner, M., Schrittwieser, S., Wondracek, G. and Weippl, E. (2011) 'Social snapshots: digital forensics for online social networks', *Proceedings of the 27th Annual Computer Security Applications Conference*, pp.113–122.

Islam, M.J., Mahin, M., Khatun, A., Debnath, B.C. and Kabir, S. (2019) 'Digital forensic investigation framework for internet of things (IoT): a comprehensive approach', *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, IEEE, pp.1–6.

Kebande, V.R. and Ray, I. (2016) 'A generic digital forensic investigation framework for internet of things (IoT)', *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, IEEE, pp.356–362.

Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006a) 'Guide to integrating forensic techniques into incident response', *NIST Special Publication*, Vol. 10, No. 14, pp.800–886.

Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006b) *SP 800-86. Guide to Integrating Forensic Techniques into Incident Response*.

Khan, A.A., Laghari, A.A. and Awan, S.A. (2021a) *Machine Learning in Computer Vision: A Review*.

Khan, A.A., Laghari, A.A., Awan, S. and Jumani, A.K. (2021b) 'Fourth industrial revolution application: network forensics cloud security issues', *Security Issues and Privacy Concerns in Industry 4.0 Applications*, pp.15–33.

Khan, A.A., Laghari, A.A., Liu, D.S., Shaikh, A.A., Ma, D.A., Wang, C.Y. and Wagan, A.A. (2021c) 'EPS-ledger: blockchain hyperledger sawtooth-enabled distributed power systems chain of operation and control node privacy and security', *Electronics*, Vol. 10, No. 19, p.2395.

Khan, A.A., Shaikh, A.A., Cheikhrouhou, O., Laghari, A.A., Rashid, M., Shafiq, M. and Hamam, H. (2021d) 'IMG-forensics: multimedia-enabled information hiding investigation using convolutional neural network', *IET Image Processing*.

Khan, A.A., Uddin, M., Shaikh, A., Laghari, A.A. and Rajput, A. (2021e) 'MF-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture', *IEEE Access*.

Khan, S., Shiraz, M., Abdul Wahab, A.W., Gani, A., Han, Q. and Bin Abdul Rahman, Z. (2014) 'A comprehensive review on adaptability of network forensics frameworks for mobile cloud computing', *The Scientific World Journal*, Vol. 2014.

Kumar, V., Laghari, A.A., Karim, S., Shakir, M. and Brohi, A.A. (2019) 'Comparison of fog computing & cloud computing', *International Journal of Mathematical Sciences and Computing (IJMSC)*, Vol. 5, No. 1, pp.31–41.

Laghari, A.A., He, H., Halepoto, I.A., Memon, M.S. and Parveen, S. (2017) 'Analysis of quality of experience frameworks for cloud computing', *IJCSNS*, Vol. 17, No. 12, p.228.

Laghari, A.A., He, H., Shafiq, M. and Khan, A. (2016) 'Assessing effect of cloud distance on end user's quality of experience (QoE)', *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, IEEE, pp.500–505.

Li, S., Qin, T. and Min, G. (2019) 'Blockchain-based digital forensics investigation framework in the internet of things and social systems', *IEEE Transactions on Computational Social Systems*, Vol. 6, No. 6, pp.1433–1441.

Loebbecke, C., Thomas, B. and Ullrich, T. (2012) 'Assessing cloud readiness at continental AG', *MIS Quarterly Executive*, Vol. 11, No. 1.

Manral, B., Somani, G., Choo, K-K.R., Conti, M. and Gaur, M.S. (2019) 'A systematic survey on cloud forensics challenges, solutions, and future directions', *ACM Computing Surveys (CSUR)*, Vol. 52, No. 6, pp.1–38.

Martini, B. and Choo, K-K.R. (2012) 'An integrated conceptual digital forensic framework for cloud computing', *Digital Investigation*, Vol. 9, No. 2, pp.71–80.

Martini, B. and Choo, K-K.R. (2014) 'Cloud forensic technical challenges and solutions: a snapshot', IEEE *Cloud Computing*, Vol. 1, No. 4, pp.20–25.

Masmoudi, F., Sellami, M., Loulou, M. and Kacem, A.H. (2017) 'From event to evidence: an approach for multi-tenant cloud services' accountability', *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, IEEE, pp.1082–1089.

Masood, A., Sharif, M., Yasmin, M. and Raza, M. (2014) 'Virtualization tools and techniques: Survey', *Nepal Journal of Science and Technology*, Vol. 15, No. 2, pp.141–150.

Math, S., Tam, P. and Kim, S. (2021) 'Intelligent media forensics and traffic handling scheme in 5G edge networks', *Security and Communication Networks*.

McKemmish, R. (1999) *What is Forensic Computing?*, Australian Institute of Criminology, Canberra.

Middleton, B. (2017) *A History of Cyber Security Attacks: 1980 to Present*, CRC Press.

Moussa, A.N., Ithnin, N., Almolhis, N. and Zainal, A. (2019) 'A consumer-oriented cloud forensic process model', *2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC)*, IEEE, pp.219–224.

Mukherjee, M., Ferrag, M.A., Maglaras, L., Derhab, A. and Aazam, M. (2020) 'Security and privacy issues and solutions for fog', *Fog and Fogonomics: Challenges and Practices of Fog Computing, Communication, Networking, Strategy, and Economics*, pp.353–374.

Nanda, S. and Hansen, R.A. (2016) 'Forensics as a service: three-tier architecture for cloud based forensic analysis', *2016 15th International Symposium on Parallel and Distributed Computing (ISPDC)*, IEEE, pp.178–183.

NIST Cloud Computing Forensic Science Working Group (2018) *NIST Cloud Computing Forensic Science Challenges*, No. NIST Internal or Interagency Report (NISTIR) 8006 (Draft), National Institute of Standards and Technology.

Pandi, G.S. and Wandra, K.H. (2018) 'Cloud forensic frameworks, challenges, state of art and future directions', *J. Emerg. Technol. Innovative Res.*, Vol. 5, No. 5, pp.712–721.

Peng, L., Luo, J. and Li, J. (2020) 'Information fusion-based digital forensics framework in cloud environment', *2020 3rd International Conference on Artificial Intelligence and Big Data (ICAIBD)*, IEEE, pp.279–283.

Pichan, A., Lazarescu, M. and Soh, S.T. (2015) 'Cloud forensics: technical challenges, solutions and comparative analysis', *Digital Investigation*, Vol. 13, pp.38–57.

Pichan, A., Lazarescu, M. and Soh, S.T. (2018) 'Towards a practical cloud forensics logging framework', *Journal of Information Security and Applications*, Vol. 42, pp.18–28.

Prakash, V., Williams, A., Garg, L., Savaglio, C. and Bawa, S. (2021) 'Cloud and edge computing-based computer forensics: challenges and open problems', *Electronics*, Vol. 10, No. 11, p.1229.

Raju, B.K.S.P.K., Moharil, B. and Geethakumari, G. (2016) 'FaaSeC: enabling forensics-as-a-service for cloud computing systems', *Proceedings of the 9th International Conference on Utility and Cloud Computing*, pp.220–227.

Rani, R., Kumar, N., Khurana, M., Kumar, A. and Barnawi, A. (2021) 'Storage as a service in fog computing: a systematic review', *Journal of Systems Architecture*, p.102033.

Razaque, A., Aloqaily, M., Almiani, M., Jararweh, Y. and Srivastava, G. (2021) 'Efficient and reliable forensics using intelligent edge computing', *Future Generation Computer Systems*, Vol. 118, pp.230–239.

Reddy, N. (2019) 'Cloud forensics', *Practical Cyber Forensics*, pp.241–275, Apress, Berkeley, CA.

Roussev, V. and Richard III, G. (2004) 'Breaking the performance wall – the case for distributed digital forensics', *Digital Investigation*.

Roussev, V., Wang, L., Richard, G. and Marziale, L. (2009) 'A cloud computing platform for large-scale forensic computing', *IFIP International Conference on Digital Forensics*, Springer, Berlin, Heidelberg, pp.201–214.

Ruan, K., Carthy, J., Kechadi, T. and Baggili, I. (2013) 'Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results', *Digital Investigation*, Vol. 10, No. 1, pp.34–43.

Ruan, K., Carthy, J., Kechadi, T. and Crosbie, M. (2011) 'Cloud forensics', *IFIP International Conference on Digital Forensics*, Springer, Berlin, Heidelberg, pp.35–46.

Sarkar, S. and Das, S. (2014) 'A state level policy framework for integrating DFaaS with e-governance', *2014 International Conference on Parallel, Distributed and Grid Computing*, IEEE, pp.153–158.

Selamat, S.R., Yusof, R. and Sahib, S. (2008) 'Mapping process of digital forensic investigation framework', *International Journal of Computer Science and Network Security*, Vol. 8, No. 10, pp.163–169.

Shalaginov, A., Iqbal, A. and Olegård, J. (2020) 'IoT digital forensics readiness in the edge: a roadmap for acquiring digital evidences from intelligent smart applications', *International Conference on Edge Computing*, September, Springer, Cham, pp.1–17.

Shvachko, K., Kuang, H., Radia, S. and Chansler, R. (2010) 'The Hadoop distributed file system', *2010 IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST)*, IEEE, pp.1–10.

Simou, S., Kalloniatis, C., Kavakli, E. and Gritzalis, S. (2014a) 'Cloud forensics: identifying the major issues and challenges', *International Conference on Advanced Information Systems Engineering*, Springer, Cham, pp.271–284.

Simou, S., Kalloniatis, C., Kavakli, E. and Gritzalis, S. (2014b) 'Cloud forensics solutions: a review', *International Conference on Advanced Information Systems Engineering*, Springer, Cham, pp.299–309.

Soltys, M. (2020) *Cybersecurity in the AWS Cloud*, arXiv preprint arXiv:2003.12905.

Spiekermann, D., Keller, J. and Eggendorfer, T. (20017) 'Using open source based distributed agents to perform digital investigation in virtual environments', *INFORMATIK 2017*.

Srinivasan, A. and Ferrese, F. (2019) 'Forensics-as-a-Service (FaaS) in the state-of-the-art cloud', *Security, Privacy, and Digital Forensics in the Cloud*, p.321.

Srivastava, P. and Choudhary, A. (2020) 'Evolving evidence gathering process: cloud forensics', *Proceedings of International Conference on Big Data, Machine Learning and Their Applications*, Springer, Singapore, pp.227–243.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E. and Markakis, E.K. (2020) 'A survey on the internet of things (IoT) forensics: challenges, approaches and open issues', *IEEE Communications Surveys & Tutorials*.

Taylor, M., Haggerty, J., Gresty, D. and Lamb, D. (2011) 'Forensic investigation of cloud computing systems', *Network Security*, Vol. 2011, No. 3, pp.4–10.

Taylor, R.W., Fritsch, E.J. and Liederbach, J. (2014) *Digital Crime and Digital Terrorism*, Prentice Hall Press.

Teing, Y-Y., Dehghantanha, A., Choo, K-K.R., Dargahi, T. and Conti, M. (2017) 'Forensic investigation of cooperative storage cloud service: Symform as a case study', *Journal of Forensic Sciences*, Vol. 62, No. 3, pp.641–654.

Van Baar, R.B., van Beek, H.M.A. and van Eijk, E.J. (2014) 'Digital forensics as a service: a game changer', *Digital Investigation*, Vol. 11, pp.S54–S62.

Van Beek, H.M.A., van Eijk, E.J., van Baar, R.B., Ugen, M., Bodde, J.N.C. and Siemelink, A.J. (2015) 'Digital forensics as a service: game on', *Digital Investigation*, Vol. 15, pp.20–38.

Xu, S., Ning, J., Li, Y., Zhang, Y., Xu, G., Huang, X. and Deng, R. (2020) 'Match in my way: fine-grained bilateral access control for secure cloud-fog computing', *IEEE Transactions on Dependable and Secure Computing*.

Yaqoob, I., Hashem, I.A.T., Ahmed, A., Kazmi, S.M.A. and Hong, C.S. (2019) 'Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges', *Future Generation Computer Systems*, Vol. 92, pp.265–275.

Yassin, W., Abdollah, M.F., Ahmad, R., Yunos, Z. and Ariffin, A. (2020) 'Cloud forensic challenges and recommendations: a review', *OIC-CERT Journal of Cyber Security*, Vol. 2, No. 1, pp.19–29.

Zargari, S. and Benford, D. (2012) 'Cloud forensics: concepts, issues, and challenges', *2012 Third International Conference on Emerging Intelligent Data and Web Technologies*, IEEE, pp.236–243.

Zawoad, S. and Hasan, R. (2013) *Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems*, arXiv preprint arXiv:1302.6312.

Zawoad, S., Dutta, A.K. and Hasan, R. (2013) 'SecLaaS: secure logging-as-a-service for cloud forensics', *Proceedings of the 8th ACM SIGSAC symposium on Information, Computer and Communications Security*, pp.219–230.

Zawoad, S., Hasan, R. and Skjellum, A. (2015) 'OCF: an open cloud forensics model for reliable digital forensics', *2015 IEEE 8th International Conference on Cloud Computing*, IEEE, pp.437–444.

Notes

1 https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g.

2 https://www.marketsandmarkets.com/PressReleases/digital-forensics.asp.

Abbreviations

DF	Digital forensics
CPS	Cloud service provider
NIST	National Institute of Standard and Technology
FaaS	Forensics-as-a-service
SaaS	Software-as-a-service
PaaS	Platform-as-a-service
IaaS	Infrastructure-as-a-service
DoS	Denial of service
DDoS	Distributed denial of service
DC	Distributed computing
DFaaS	Distributed forensics-as a-service
CF	Cloud forensics
IoT	Internet of things
EC2	Elastic computer cloud

EBS	Elastic block storage
GFS	Google file systems
DFS	distributed file system
HDFS	Hadoop
VM	Virtual machine
VMM	Virtual machine monitor
AWS	Amazon Web Services