Asian Journal of Research in Computer Science

Volume 16, Issue 1, Page 1-14, 2023; Article no.AJRCOS.100348
ISSN: 2581-8260

Cloud Computing Forensics; Challenges and Future Perspectives: A Review

Burak Cinar [a*] and Jasmin Praful Bharadiya [b]

[a] ThinkSecure Inc., Turkiye.
[b] University of the Cumberlands, United States.

Authors' contributions

This work was carried out in collaboration between both authors. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2023/v16i1330

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/100348

Review Article

Received: 17/03/2023
Accepted: 19/05/2023
Published: 24/05/2023

ABSTRACT

Cloud computing has become increasingly popular in recent years, evolving into a computing paradigm that is both cost-effective and efficient. It has the potential to be one of the technologies that has had the most significant impact on computing throughout its history. Regrettably, cloud service providers and their customers have not yet developed major forensic tools that can assist with the investigation of criminal conduct that occurs in the cloud. Because it is difficult to prevent cloud vulnerabilities and criminal targeting, it is necessary to be aware of how digital forensic investigations of the cloud may be carried out. This is because cloud vulnerabilities and criminal targeting are difficult to avoid. In this context, the current study examines current and future trends in cloud forensics, methodology for cloud forensics, and cloud forensic tools. In addition, the study also looks at cloud forensic approaches.

Keywords: Cloud computing; cloud forensic; forensic tools; software as a service.

**Corresponding author: Email: burak@thinksecure.io;*

1. INTRODUCTION

Since it was first created, the cloud has not undergone any major changes or shown any substantial progress in a number of key areas [1]. The concept of cloud computing is the way of the future, and it will provide significant economic benefits to enterprises. The introduction of cloud computing has ushered in a host of novel prospects, some of which lend themselves more favorably than others [2]. As a result of this expansion, new challenges and dangers have emerged that might pose a threat to organizations, as cloud computing has developed into a new battleground for cybercrime [3]. Users with malicious intent are able to exploit serious security holes that exist in the cloud. The majority of the functionality of cloud goods may be accessible by remotely accessing virtual computers, performing the duties associated with those functions, and then deleting the virtual machines [4]. This is possible because cloud products do not require consumers to physically own the infrastructure. As the use of the cloud became more widespread, the number of cloud critics also rose [5]. The investigation of crimes committed in the cloud takes a somewhat different approach than that taken in regular settings. During the course of the prior decade's worth of research, a great number of forensics fields, including trust, network forensics, evidence collecting, privacy, and data provenance, came into existence. Investigators that specialize in digital forensics have a unique challenge when confronted with this kind of computing [6]. In addition to this, it highlights the significance of the development of specialized forensic tools for the purpose of gathering and analyzing digital evidence in the digital world, sometimes even before the evidence is destroyed entirely, including a variety of service models and structural configurations [7]. In order to get complete access to and control over the dispersion of cloud resources, digital forensic investigators have been presented with additional obstacles as a result of these factors. In computing, the term "virtualization" refers to operating systems that run atop another operating system as if they were running on their hardware. As a result of virtualization, cloud computing came into being [8, 9]. The development of new computer paradigms like these paves the way for new forms of cybercrime. These methods may not be instantly usable in the cloud, despite the fact that research efforts in digital forensics for classic computer paradigms including virtual environments have showed improved outcomes. User data is dispersed and frequently resides in locations that are not accessible to forensics investigators while working in a cloud setting. The next portions of this article are organized as follows: first, an explanation of recent and upcoming developments in cloud forensics is provided, then a review of tools and methods for cloud forensics is provided, and lastly, incident management in the cloud is presented [10].

Today, businesses are becoming more aware of the benefits of cloud computing and are moving towards transferring their data to the cloud. This shift attracts the interest of cyber thieves, who pose a greater risk to cloud resources due to the increased degree of risk associated with them [11]. The fact that the size of an average digital forensic case is expanding at a pace of 35% per year demonstrates the rapid surge in the number of digital crimes [12]. Therefore, it is of the utmost need to place a greater emphasis on cloud computer security and, as a direct result of this, cloud computing forensic investigation. It should come as no surprise that having a fundamental understanding of both digital forensic investigation and cloud systems is essential in order to have a conversation about either topic [13-17].

According to the definition provided by the United States National Institute of Standards and Technology (NIST), cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [18-20]. In today's world, cloud computing can be broken down into three primary categories of service: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Infrastructure as a service (IaaS) offers customers a virtualized machine, which is an environment similar to that of a physical machine but with some limitations. Platform as a service (PaaS) typically offers customers access to an Application Programming Interface (API) [21-24].

2. OVERVIEW OF CLOUD COMPUTING

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Users can access the services over the internet at any time and from any location by using a thin client, such as a web browser. Let's call it Cloud A. The ability to scale up or down computational needs in line with client requirements. The ability to access a network at any time and from any location is referred to as connectivity. Multi-tenancy is the ability to accommodate several tenants on the same set of physical resources, including shared network connections, memory, and storage space. Visibility is the ability for customers to fully understand and manage the specifications, use, and prices of their cloud deployments. Measured service is the ability to charge consumers according to how much of the offered items they really utilize [25-30].

The various advantages of cloud computing have contributed significantly to its rapid growth. The main benefit of cloud computing is the possibility of realizing economies of scale due to the flexible and effective use of resources available as well as specialization. Cloud computing offers a wide range of deployment and service delivery options. Public cloud deployment is one of the deployment strategies. This method uses the internet to make computer tools and services available to the general populace. A cloud that is owned and managed by a separate third party and offers cloud services is referred to as a public cloud [12]. A private cloud is a computer environment that a firm owns and controls entirely, either internally or through a third party. Private clouds are created to support a single tenant and, by their very nature, allow more control over all of the computing resources [31]. As an alternative to private cloud computing, community cloud involves the pooling and sharing of data storage and processing capacity across several companies that uphold the same privacy, security, and other legal criteria. A hybrid cloud is a combination of two or more clouds that are connected via standardised or proprietary technologies to enable interoperability. 1. Software-as-a-service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS) are three paradigms for cloud services that are widely accepted, according to Jansen and Grance (2011) [32, 33]. Software-as-a-service (SaaS) is a method of deploying software in which one or more applications are made available for usage on demand as a turnkey service that can be accessed through a thin client together with the computing resources necessary to operate them. This strategy aims to reduce the overall cost of creating hardware and software, as well as that of maintaining and using them. In this paradigm, consumers have very limited rights, such as the ability to alter application settings and their personal data, but CSPs have total authority over the apps and the underlying infrastructure. Platform-as-a-Service, or PaaS for short, is a method of deploying software in which the computing platform is made available as an on-demand service and is then used as the basis for developing and deploying applications [34]. Its main goal is to make acquiring, setting up, and managing the platform's underlying hardware and software components—such as databases, operating systems, and development tools—more straightforward, hence minimising costs and complexity. IaaS, or infrastructure-as-a-service, is a software deployment paradigm in which the essential components of a computer system, such as servers, software, and networking hardware, are made available as a service that can be accessed whenever it is needed. This method enables the construction of a foundation for the development and execution of applications. Because they obtain those resources in the form of virtualized objects that can be managed through a service interface, customers of infrastructure as a service don't need to worry about purchasing, storing, or managing basic hardware and software infrastructure components [35-39].

3. AN INTRODUCTION TO CLOUD FORENSICS

Cloud forensics can be defined as the use of digital forensics on cloud computing platforms. Interdisciplinary research is being done in this area. The newly formed NIST cloud forensic working group came up with the following definition [40]: "Cloud Computing forensic science is the application of scientific principles, technological practises, and derived and proven methods to process past cloud computing events through identification, collection, preservation, examination, and reporting of digital data for the purpose of facilitating the reconstruction of these events." The CSPs swapping services makes it more challenging to follow the development of events and further complicates the issue. As a result, the forensics procedure that would be appropriate in a traditional setting (one that does not use cloud computing) would not apply here.

The technical, organisational, and legal dimensions make up cloud forensics [41]. The forensic investigation process in the context of cloud computing necessitates the use of specific techniques and tools, which are referred to as the technical dimension as a whole. This includes activities like data gathering, real-time forensics, separating evidence, and preventative actions. The organisational component, on the other hand, looks at the forensics aspects that have to do with organisation. The sorts of participants that are included include CSPs, clients, legal counsel, and issue handlers. It also covers things like legally binding service level agreements (SLAs), rules, and regulations [41,42]. Last but not least, the legal aspect includes the creation of rules and agreements to guarantee that forensic activities don't break the laws and regulations in the countries where the data is stored or collected, while also protecting the privacy of co-tenants who share the same infrastructure. This is achieved by making sure that forensic procedures don't violate the rules and laws of the countries where the data is stored or gathered [43].

4. STEPS IN CLOUD FORENSIC [43-48]

- **Analysis:** When carrying out an investigation using cloud forensics, the processes that follow are carried out.
- **Identification:** This step involves the examiners determining whether or not there has been possibly harmful activity or improper behavior inside the cloud-based services. A suspicious event in the cloud, a complaint from an individual, abnormalities discovered by an intrusion detection system, monitoring and profiling as a result of an audit trail all qualify as examples of these activities.
- **Preservation and Collection:** In this stage, data is gathered from all available sources in a way that does not compromise its integrity in compliance with forensic and legal criteria. For the sake of a future investigation, every piece of information and piece of evidence has been stored away safely. There is a possibility that the gathering of data may need for the storing of very large volumes of data. As a consequence of this, investigators are obligated to consider the laws and regulations that regulate data protection and privacy, as well as the consequences these laws and regulations have for evidence that is stored in the cloud. When obtaining data from the cloud vendor side, you should at all times take into consideration the data of any other users or organizations. An accurate representation of the data stored in the cloud must be gathered before continuing the investigation. An investigator can attempt to get and keep data saved in the cloud by serving the cloud service provider with a court order.
- **Detection:** After the data have been gathered, a number of different approaches and algorithms (such as filtering and pattern matching, for example) are utilised in order to discover any potentially harmful code or suspicious patterns of behaviour.
- **Analysis:** After detection comes the process of using forensic methods to evaluate and investigate the data as well as the crime that was committed. In order to collect evidence, legal authorities may direct the investigation to either an organisation or an individual. After doing an analysis of the data, the testimony has to be communicated to law enforcement personnel as well as the victim organisation or individual.
- **Presentation**: This is the final step, which involves presenting evidence that was obtained in front of a judge or other legal official. This is performed by the utilisation of a report that has been appropriately produced, in which the findings are required to be offered by testimonies on the subject that was researched.
- **Documentation:** It is challenging to convince the court that the evidence gathered throughout the investigation was properly documented and that there were no alterations made to the evidence during the earlier stages of the procedure.

5. IS CLOUD COMPUTING A POSSIBLE RAY OF SUNSHINE OR A LOOMING STORM?

Cloud computing aspires to the concept of computers as a utility, much like the provision of services like water, gas, electricity, and telephones. It also symbolizes the desire to use computational resources to provide real services. Software, the computing platform, and the computing infrastructure can all be conceived of as services without considering how or where they are really provided. This is due to the fact that there is no distinction between the three.

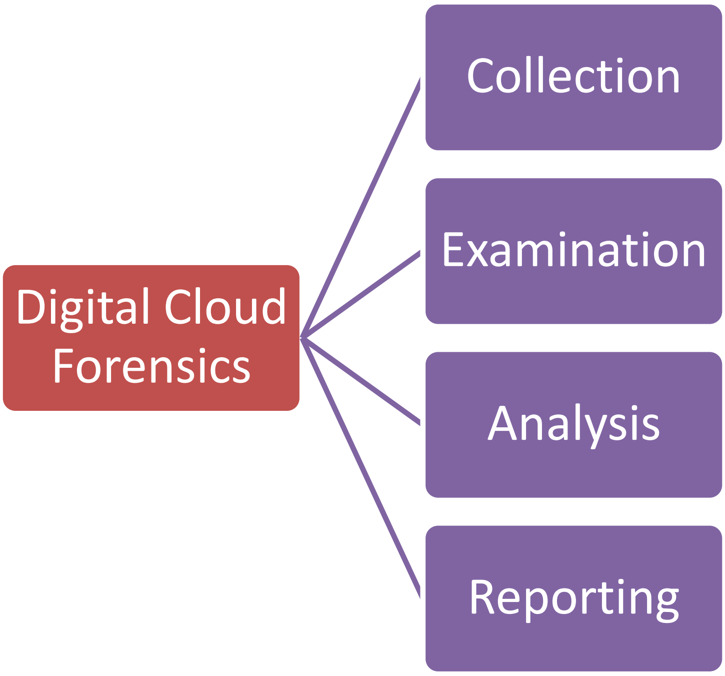

Fig. 1. Steps in digital cloud forensics

Major industry players have realized the potential of cloud computing, as evidenced by the fact that each of the top five software companies in terms of sales revenue has a sizable cloud product portfolio. Although there is a lot of material in the community that illustrates the basic concepts, the phrase "cloud computing" is not yet understood by everyone. Several authors have put forth the idea that cloud computing is a development of cluster computing. Cloud computing is more precisely known as cluster computing with software as a service [49-53]. There are five key characteristics of cloud computing, three delivery options, and four deployment model. This is a concept that is simple to comprehend. As of this writing, perspectives on whether cloud computing might promote or oppose computer forensics investigations are rather divided. One group of people thinks cloud computing might support such inquiries, while the other group thinks it will hinder them. In the next section, we will analyze both the good and bad elements of the topic in more detail after providing a high-level summary of both sides of the argument [54-56]. On the one hand, in order to accommodate investigations conducted on cloud-based systems, the computer forensic process model would need to be modified and a new set of procedures would need to be put in place. On the other hand, using the resources and services made available by cloud computing might be advantageous for computer forensic investigations in order to support the inquiry [57, 58]. The main benefit of cloud computing is its capacity for centralising data storage; having all of one's data in one place enhances forensic readiness, which in turn leads to a quicker and more well-coordinated response to crises. When IaaS providers have access to centralised data, they can build a dedicated forensic server within the cloud. When needed, this server is available for usage. The services and resources that cloud computing platforms may offer, or, more precisely, the scope and power of these services, confer further benefits to the discipline of computer forensics. A huge advantage for the computer forensic investigator is the availability of potentially petabytes of storage and highly available compute-intensive tools. These two elements both influence the research process. During the course of an investigation, a detective may gather a lot of images of hard discs. Infrastructure as a Service, or IaaS, might potentially be used to store these pictures on the cloud. Second, forensic investigators may use the high availability compute intensive resources for compute-intensive activities [59,60]. Forensic investigators, for example, may need to break passwords or encryption keys or review a large number of photos, all of which may be time-consuming and taxing on a computer's processing power and memory [61, 62]. For instance, an MD5 hash is created when a piece of data is stored in Amazon S3. This indicates that it is no longer necessary to generate the time-consuming MD5 checksums that were previously required. The various log files that might be discovered on a computer can be a useful source of information during a forensic examination. However, logging is occasionally treated as an afterthought, and as a result, either insufficient disc space is provided or no logging occurs at all. Due to the scale at which cloud storage is being used, logging may be done, configured to the proper level, and logs can be made available upon request. This is made feasible by the cloud's scalability [62, 63]. A C2 audit trail represents the enhanced logging capabilities of modern operating systems. However, due to worries that it can impede performance and increase log volume, this option is rarely used. Better logging may be achieved with cloud computing, and the granularity of logging can be changed to suit specific needs. Virtualization, which has been considered differently as both a benefit and a drawback, is the final area of concern. As was previously said, in cloud computing settings, virtualization is used to enable several users to use the same resources. Software, platforms, and infrastructure are just a few of the many resources that may all be virtualized. It was also highlighted that for forensically sound data collection to take place, a bit-by-bit copy of a disc image must be made using the required software. It takes extra effort and time to record memory images during live investigations because memory must be frozen before the host being copied loses power. However, in a virtual environment, these steps are unnecessary because administrative tools like snapshots and other functionality make it easy to take photos of the disc and memory. However, law enforcement authorities (i.e., the guidelines set by ACPO) have not yet determined the forensic validity of this form of acquisition. When considered from a forensic angle, data collecting is cloud computing's worst drawback. This is the procedure of locating the precise location of data storage and then physically retrieving it. The search and seizure tactics used in the traditional computer forensic process are not feasible since evidence is kept in cloud datacenters. These methods are used to gather evidence. Additionally, it is exceedingly difficult, if not impossible, to maintain a chain of custody in relation to the collection of the evidence [64]. It is nearly hard for investigators to adhere to the ACPO advice since employing cloud computing makes it difficult, if not impossible, to uphold ACPO standards. The cloud computing is to blame for this [65]. The four guiding principles for the procedures and level of knowledge required for evidence management are laid forth in the ACPO manual. These requirements cannot be met since clouds function as remote datacenters, making the ACPO advice unnecessary. The validity, integrity, and admissibility of the evidence in a British court process would thus be called into doubt as a result of this [66]. There is a general loss of control over the course of the forensic investigation since the data are being stored somewhere else where access to them is not possible. Overall, this is the situation. Due to a lack of knowledge on the precise place where data is held, this makes it harder to put together a sequence of events and build a timeline. This in turn makes it more difficult to recreate a crime scene. A variety of other issues that will be discussed in more depth further down the page can potentially hinder the study. The gathering of data and the loss of control are two drawbacks. the disposal of important objects, some of which would have served as key pieces of evidence. In cloud datacenters, it could be difficult, if not impossible, to access items like registry entries, temporary files, and RAM (often because virtualization is utilised) [67-69]. There is a potential that the metadata will be lost when data is downloaded from the cloud. It is useful for the investigator to have access to metadata, such as the times the file was created, edited, and accessed, while performing a forensic investigation. Many investigators still prefer to carry out their own authentication rather than depending on the cloud storage service's hash authentication, even though certain cloud storage providers, including Amazon S3, do offer a mechanism to confirm data (using MD5 checksums). This occurs as a result of the inconsistency of cloud storage services. Another restriction is the absence of tool support at the moment for using cloud datacenters. Although computer forensics is still a young subject of study, it has advanced to the point where tools are suitable for handling typical localised investigations [70-72]. The forensic investigator may utilise instruments like EnCase, Helix, and FTK to help with tasks like the initial data gathering all the way through the process of producing written evidence that is acceptable in a court environment. The forensic investigator can utilise various instruments to help them with these duties. The last concern is one that results from computer forensics' legal and ethical components. This problem results from the requirement that all digital evidence gathered during an inquiry be presented to a jury, who will subsequently render a verdict on the matter. In conventional computer forensics, the investigators must present their findings to the jury. As a result, investigators frequently find themselves in the awkward position of having to describe how evidence was gathered and what it suggests about the case in terms that are unique to their discipline. Working with conventional, locally based computer systems can make this challenging, let alone cloud datacenters, which may be thousands of miles away, run 40,000 virtual machines (VMs) across 512 servers, and are accessed by 1000 tenants, of which the accessed is one. This may just be too much information for the ordinary juror to process given that they only have a basic grasp of how to utilise a home computer [73-75].

6. THE CHALLENGES CLOUD FORENSICS FACES

As you may have guessed, there are a number of particular challenges specific to the subject of cloud forensics. The challenges posed by cloud forensics involve both technological and legal issues [76]. Some potential issues in conducting a forensic investigation in the cloud include the following:

- Issues with the user's home jurisdiction Cloud services are commonly hosted in states or nations other than the user's location. There are times when users can choose this location, but it's not always the case. The world is home to many cloud servers. For instance, Google has them across Australia, Europe, Asia, North and South America. This might make determining which jurisdiction has jurisdiction over the offence more challenging [77].
- Unstable: When performing traditional digital forensics investigations, the IT environment is usually "frozen" to avoid interruptions or new issues while investigators complete their work. To make sure the probe goes off without a hitch, this is done. On the other hand, because public cloud providers may serve hundreds of thousands or millions of users, this is often not possible. Instead, the environment is still dynamic and open to change, making it potentially unstable [78].
- Physical access: There are some instances in which physically inspecting a cloud server can be helpful with forensics. However, this can be difficult to accomplish with large cloud providers because they implement stringent security regulations to prevent unauthorised individuals from entering the premises. In addition to this, as was mentioned earlier, there is no guarantee that the cloud server will be physically located close to the investigator [79].

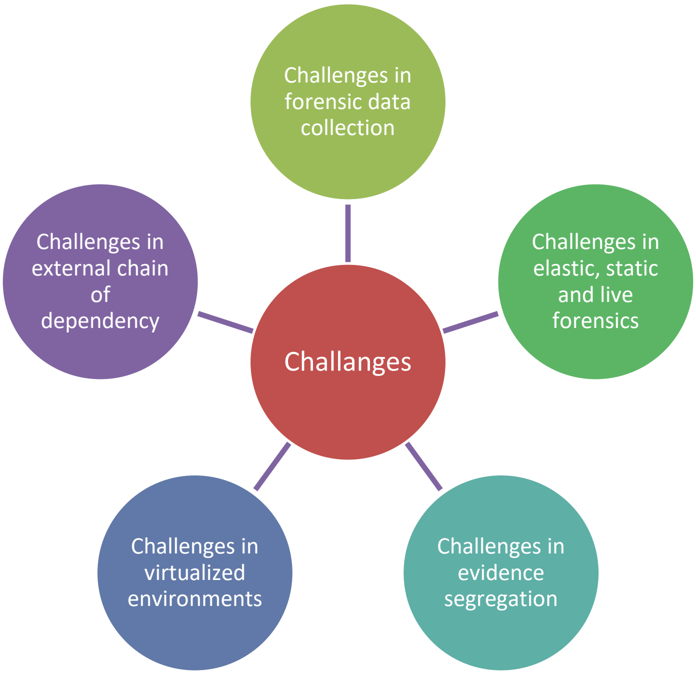
Challenges in forensic data collection
Challenges in external chain of dependency
Challenges in elastic, static and live forensics
Challanges
Challenges in virtualized environments
Challenges in evidence segregation

Fig. 2. Challenges

- Decentralisation: In order to boost data availability and reliability, cloud companies commonly store files across numerous servers or data centres. This decentralisation and fragmentation make it more difficult to detect the problem and undertake forensics [80].
- Data that is either unavailable or deleted: The information that cloud providers provide to investigators may vary. For instance, log files may not be accessible in some cases. In addition, if the crime caused data to be deleted, it becomes difficult to reconstruct this data, determine who its owner is, and use it in cloud forensic analysis [81].

7. WHAT'S HOT RIGHT NOW AND WHAT'S UP NEXT FOR CLOUD FORENSICS

Digital forensics, network forensics, and hardware forensics are only a few of the many different forms of forensic investigation that collectively go under the umbrella phrase "cloud forensics" [82]. Various cloud stakeholders (such as cloud providers, cloud customers, cloud brokers, cloud carriers, and cloud auditors) must interact with one another in order to simplify internal and external investigations. Basic features of cloud computing include a high degree of virtualization, data duplication, jurisdiction, and multi-tenancy. These characteristics increase the complexity of cloud forensics to various degrees [83]. Due to the apparent resources it gives, as well as its low cost, wide availability, and flexibility, cloud forensics have become widely used in the area of forensics. There are several options for database security, software integration, and application development in this area of cloud forensics, which also includes private, hybrid, and public models [84-86]. Governments and organisations of all sizes may benefit from a variety of advantages thanks to cloud computing, including high scalability, decreased IT expenses, backup, and speedy installation [1]. Similar to this, in order to achieve the objectives of low latency and scalability, cloud-based telecommunications service providers are moving their data centres to a range of various geographic locations. The rise in online criminal behaviour and the broadening impact of cloud computing, however, pose a more significant threat. Security experts have expressed concern about how challenging cloud forensics are to do. Cybercriminals' main objective is to take advantage of the cloud's existing weaknesses. An example of a potential application in the field of digital forensics is an external inquiry conducted in a cloud-based environment [87,88]. In this area, events in the cloud are processed and the results are retrieved using academic standards and norms, conventional practises, and cutting-edge technology. Additionally, cloud storage offers a wide range of virtualization, replication, and multi-tenancy capabilities. Additionally, the technique used in cloud forensics depends on how the software platform is installed and operates. There are a lot fewer possibilities for monitoring techniques and services in Platform as a Service (PaaS) and Software as a Service (SaaS) implementations [89-93].

Despite the complexity of cloud forensics, it is certain that the growth of cloud computing has led to concerns about users' security and privacy. Many of the currently hired forensics officers have witnessed a significant increase in their engagement in authorization, authentication, and accounting (AAA) as a result of the advent of cloud technology. This is so that malicious assaults may be looked into and identified using digital proof. It has a high degree of precision and contrasts sharply with other forensic techniques that employ the data, making it equivalent to traditional forensic methods for extracting evidence from log data. Legal, organisational, and technological forensics are the three subcategories that make up forensics in the cloud. Laws and agreements have been made to offer this guarantee that digital forensic methods do not violate the rules that regulate their usage [94,95]. Instead, a wide range of factors of corporate policy are involved in the organisation of computer forensics [96]. Last but not least, the technological scope describes the procedures and methodologies that will be used to conduct a cloud investigation. Cloud forensics has become a regular procedure in the field of digital forensics as a direct result of this. It facilitates the use of forensics as an investigative tool by integrating cloud capabilities like remote analysis, monitoring, and scaling, such as the ability to manage huge workloads. Now, forensics may be employed as a research tool.

Cloud Computing Predicted Developments and Changes: A multi-tenancy cloud trust model with quality of service monitoring. The Multi-Tenancy Cloud trust model with Quality of Service (QoS) focuses mostly on the Infrastructure as a Service (IaaS) platform. The model demonstrates why it is crucial to give cloud solution users a way to assess the dependability and quality of the services offered by cloud service providers before to signing up for such services. The suggested approach requires ongoing, real-time monitoring of service quality. In addition to fostering consumer confidence and ensuring that clients sign up for cloud services that fulfil specific criteria and metrics, this makes it easier to evaluate cloud service providers.

Security for Logging Service provided: In order to undertake investigations that help expose unlawful or fraudulent activities perpetrated by rivals and aid in their prosecution, logs in cloud infrastructures are crucial [97]. Although cloud platforms are advantageous computing models, Zawoad et al. discovered that the computational power and storage resources made available by computer clouds might also tempt dishonest users to carry out attacks via the platforms. This realisation came about during the development of their Secure Logging as a Service model. As Zawoad et al. developed their Secure Logging as a Service approach, this was brought up [98]. Other researchers point out difficulties with using the Secure Logging as a Service Scheme (SecLaaS) to perform cloud forensics, such as a decreased degree of control when users of cloud services heavily depend on service providers to collect logs from computer clouds [99]. They explore these concerns when talking about the Secure Logging as a Service Scheme (SecLaaS). The results of this study show that relying excessively on cloud service providers might lead to a loss of confidence in their investigators, many of whom are unqualified. They caution that bad actors may manipulate the logs using their power over the created logs if cloud service providers are compromised. Additionally, they issue a warning that cloud service providers can refuse to comply with requests for all required logs if such requests clash with their own internal data protection requirements. The main goal of the proposed framework was to overcome the difficulties caused by the lack of logging standards, the erratic nature of logs, and the multi-tenancy feature of cloud platforms. These issues emerge because shared hardware, which could also store the logs of multiple other users, may be used to provide virtualized services. Architecture for the cloud with forensic capabilities Forensic Supported In order to support a trustworthy digital forensics operation on cloud systems, cloud architecture emphasises the importance of securely preserving produced logs, proof of data custody, and provenance information in addition to timestamp data [100]. According to Zawoad et al. any data collected should be accessible to cloud users, investigators, and legal authorities [101-103].

8. CONCLUSIONS

One of the most revolutionary innovations in computer history may very well be cloud computing. Both cloud service providers and users have yet to develop suitable forensic tools that may help with cloud-based criminal activity investigations.With regard to crimes using computers, mobile devices, and the Internet, computer forensics is a crucial area of computer science. Computer forensics' primary function is to carry out criminal investigations by examining any evidence discovered in digital forms. Because there have been so many recent reports of cybercrimes, it is now more important than ever to create specialised forensic tools for gathering and analysing digital evidence in the digital world, sometimes even before it has been lost or erased. Digital forensic investigators now face a greater barrier in gaining complete access to and control over the dispersed cloud resources due to the new cloud computing paradigm's distinctive architecture and variety of service models. While the present chapter begins by outlining the significance of digital forensics in general, it concentrates particularly on their function in cybercrime investigations in the digital cloud. This review defines the fundamental ideas, structures, and service paradigms of the cloud computing paradigm. The key benefits, drawbacks, difficulties, and strategies for digital forensic processes are then discussed, along with methods for supporting the isolation and preservation of any digital evidence. The review article concludes by highlighting a number of issues in cloud forensic analysis that require more study.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Amazon, AWS Security Center, Seattle, Washington. Available:aws.amazon.com/security
2. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud

Computing V2.1, San Francisco, California; 2009.
Available:www.cloudsecurityalliance.org/csaguide.pdf

3. EurActiv, Cloud computing: A legal maze for Europe, Brussels, Belgium; 2011.
Available:www.euractiv.com/en/innovation/cloud-computing-legal-maze-europe-linksdossier-502073
4. European Network and Information Security Agency, Cloud Computing: Benefits, Risks and Recommendations for Information Security, Heraklion, Crete, Greece; 2009.
Available:www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
5. Federal Bureau of Investigation, Regional Computer Forensics Laboratory, Annual Report for Fiscal Year 2007, Washington, DC.
Available:www.rcfl.gov/downloads/documents/RCFL_Nat_Annual07.pdf), 2007.
6. Gartner, Gartner says worldwide cloud services revenue will grow 21.3 percent in 2009, Stamford, Connecticut; March 26, 2009.
Available:www.gartner.com/it/page.jsp?id=920712
7. Gens F. IT cloud services forecast – 2008 to 2012: A key driver of new growth; October 8, 2008.
Available:blogs.idc.com/ie/?p=224
8. Kent K, Chevalier S, Grance T, Dang H. Guide to Integrating forensic techniques into incident response, Special Publication 800-86, National Institute of Standards and Technology, Gaithersburg, Maryland; 2006.
9. Mell P, Grance T. The NIST Definition of Cloud Computing (Draft), Special Publication 800-145 (Draft), National Institute of Standards and Technology, Gaithersburg, Maryland; 2011.
10. Meyers M, Rogers M. Computer forensics: The need for standardization and certification. International Journal of Digital Evidence. 2004;3(2).
11. Perry R, Hatcher E, Mahowald R, Hendrick S. Force.com cloud platform drives huge time to market and cost savings, IDC White Paper, International Data Corporation, Framingham, Massachusetts.
Available:thecloud.appirio.com/rs/appirio/images/IDC _Force.com_ROI_Study.pdf), 2009.
12. Beebe N. Digital forensic research: The good, the bad and the unaddressed, in Advances in Digital Forensics V, G. Peterson and S. Shenoi, Editors. Springer: Heidelberg; 2009.
13. Broadhurst R, Developments in the global law enforcement of cyber crime. Policing: International Journal of Police Strategies and Management. 2006;29.
14. Liles S, Rogers M, Hoebich M. A survey of the legal issues facing digital forensic experts, in Advances in Digital Forensics V, G. Peterson and S. Shenoi, Editors. Springer: Heidelberg; 2009.
15. Oberheide J, Cooke E, Jahanian F. CloudAV: N-version antivirus in the network cloud, in Proceedings of the Seventeenth USENIX Security Conference; 2008.
16. Roussev V, et al. A cloud computing platform for large-scale forensic computing, in Advances in Digital Forensics V, G. Peterson and S. Shenoi, Editors. Springer: Heidelberg; 2009.
17. lmulhem A, Traore I. Experience with engineering a network forensics system. In: Proc. of the 2005 Int. Conf. on Information Networking, Jeju; 2005.
18. Biggs S. Cloud computing: The impact on digital forensic investigations. In: Proc. of the 4th Int. Conf. for Internet Technology and Secured Transactions, ICITST; 2009.
19. Birk D. Technical Challenges of Forensic Investigations in Cloud Computing Environments. In: Workshop on Cryptography and Security in Clouds. 2011;1–6.
20. Catteddu D, Hogben G. Cloud computing – Benefits, risks and recommendations for information security. ENISA Technical Report; 2009.
21. Doelitzscher F, Reich C, Knahl M, Clarke N. Incident detection for cloud environments. In: EMERGING 2011, The Third International Conference on Emerging Network Intelligence. 2011; 100–105.
22. Haggerty J, Llewellyn-Jones D, Taylor M. FORWEB: file fingerprinting for automated network forensics investigations. In: Proceedings of the First International Conference on Forensic Applications and Techniques in Telecommunications Information and Multimedia eForensics; 2008.
23. Noblett MG, Pollitt MM, Presley LA. Recovering and examining computer

forensic evidence. Forensic Science Communications. 2000;2(4).

24. Ranum MJ. Network forensics and traffic monitoring. Computer Security Journal. 1997;35–39.
25. Ruan K, Carthy J, Kechadi T, Crosbie M. Cloud forensics. In: Advances in Digital Forensics VII. 2011;361:35–46.
26. Scarfone K, Mell P. Guide to intrusion detection and prevention systems. NIST Special Publication. 2007;800-94.
27. Sempolinski P, Thain D. A comparison and critique of eucalyptus, opennebula and nimbus. In: 2010 IEEE Second International Conference on Cloud Computing Technology and Science. IEEE; November 2010.
28. Shanmugasundaram K, Memon N, Savant A. ForNet: A distributed forensics network. In: Second International Workshop on Mathematical Methods. Models and Architectures for Computer Networks Security. 2003;417–426.
29. Somorovsky J, Heiderich M, Jensen M. All your clouds are belong to us: security analysis of cloud management interfaces. In: Proceedings of the ACM Cloud Computing Security Workshop, CCSW; 2011.
30. Wang HM, Yang CH. Design and implementation of a network forensics system for Linux. In: 2010 International Computer Symposium (ICS 2010). IEEE. December 2010; 390–395.
31. Garfinkel T, et al. Terra: a virtual machine-based platform for trusted computing. SIGOPS Oper. Syst. Rev. 2003;37.
32. Glavach, S. and D. Zimmerman, Cyber Forensics in the Cloud. IAnewsletter, 2011. 14.
33. Grobauer B, Schreck T. Towards incident handling in the cloud, in Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, CCSW 2010. ACM Press: New York; 2010.
34. Grobauer B, Walloschek T, Stocker E. Understanding cloud computing vulnerabilities. IEEE Security & Privacy Magazine. 2011;9.
35. Hoopes, J, et al, Virtualization for Security. 2009, Burlington: Syngress Publishing.
36. Mather T, Kumaraswamy S, Latif S. Cloud Security and privacy – an enterprise perspecive on risks and compliance. Sebastopol: O’Reilly Media; 2009.
37. Pilli ES, Joshi RC, Niyogi R. Data reduction by identification and correlation of TCP/IP attack attributes for network forensics, in Proceedings of the International Conference & Workshop on Emerging Trends in Technology, ICWET 2011. ACM Press: New York; 2011.
38. Santos N, Gummadi KP, Rodrigues R. Towards trusted cloud computing, in Proceedings of the 2009 Conference on Hot Topics in Cloud Computing, HotCloud 2009. USENIX Association: Berkeley; 2009.
39. Zafarullah AF, Anwar Z. Digital forensics for eucalyptus. In Proceedings of the, Frontiers of Information Technology, FIT 2011. IEEE Computer Society: Washington, DC; 2011.
40. Abbadi IM. Toward trustworthy clouds’ internet scale critical infrastructure. in Information Security Practice and Experience: 7th International Conference, ISPEC 2011, Guangzhou, China, May 30–June 1, 2011. Proceedings 7. Springer; 2011.
41. Abbadi IM, Lyle J. Challenges for provenance in cloud computing. in TaPP; 2011.
42. AbdElnapi N, Omara FA, Omran NF. A hybrid hashing security algorithm for data storage on cloud computing. International Journal of Computer Science and Information Security (IJCSIS). 2016;14(4).
43. Abernathey RP, et al, Cloud-native repositories for big scientific data. Computing in Science & Engineering. 2021;23(2).
44. Abiodun OI, et al A review on the security of the internet of things: challenges and solutions. Wireless Personal Communications. 2021;119:2603-2637.
45. Abiodun OI, et al. Big Data: an approach for detecting terrorist activities with people’s profiling. in proceedings of the International MultiConference of Engineers and Computer Scientists; 2018.
46. Barrett D, Kipper G. Virtualization and forensics: a digital forensic Investigator’s guide to virtual environments. Syngress; 2010.
47. Hemdan EE-D, Manjaiah DH. Exploring digital forensic investigation issues for cyber crimes in cloud computing environment. Proceeding of 1st International Conference on Computer Communication and Networks (i3CN); 2015.
48. Hemdan EE-D, Manjaiah DH. Spark-based log data analysis for reconstruction of

cybercrime events in cloud environment. 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT). IEEE; 2017.

49. Hirwani, Manish, et al. Forensic acquisition and analysis of VMware virtual hard disks. Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp); 2012.

50. Jeong D, et al. Investigation methodology of a virtual desktop infrastructure for IoT. Journal of Applied Mathematics; 2015.

51. Kebande VR, Venter HS. A cloud forensic readiness model using a Botnet as a service. The international conference on digital security and forensics (DigitalSec2014). Ostrava: The Society of Digital Information and Wireless Communication; 2014.

52. Liu, Shouqiang, et al. Research of animals image semantic segmentation based on deep learning. Concurrency and Computation: Practice and Experience. 2020;32.1:e4892.

53. Mell P, Grance T. Nist cloud computing forensic science challenges. Draft NISTIR 8006; 2014.

54. Port 4444 Details.
Available:http://www.speedguide.net/port.php?port=4444/
[last accessed 23-6-2020].

55. Rani D, Geethakumari G. An efficient approach to forensic investigation in cloud using VM snapshots. IEEE International Conference on Pervasive Computing (ICPC); 2015.

56. Simou S, et al. A meta-model for assisting a cloud forensics process. Risks and security of internet and systems. Springer International Publishing. 2015;177–187.

57. Volatility Foundation.
Available:http://www.volatilityfoundation.org /
[last accessed 23-6-2020]

58. Waldo Delport MK, Olivier MS. Isolating a cloud instance for a digital forensic investigation. in Information and Computer Security Architecture (ICSA); 2011.

59. Zafarullah Z, Anwar F, Anwar Z. Digital forensics for eucalyptus. in Proceedings of Frontiers of Information Technology (FIT). IEEE. 2011;110–116.

60. Zawoad, Shams, Ragib Hasan, Anthony Skjellum. OCF: an open cloud forensics model for reliable digital forensics. Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on. IEEE; 2015.

61. Using vmrun to control virtual machines; 2008.

62. Alqahtany S, et al. A forensic acquisition and analysis system for IaaS. Clust Comput. 2016;19.

63. Dykstra J, Sherman A. Understanding issues in cloud forensics: Two hypothetical case studies. Journal of Network Forensics; 2011. b.

64. Dykstra J, Sherman A. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques. 2012, January: DoD Cyber Crime Conference.

65. Dykstra J, Sherman AT. Design and implementation of frost: digital forensic tools for the OpenStack cloud computing platform. Digit Investig. 2013;10.

66. Hemdan EED, Manjaiah DH. Forensic analysis approach based on metadata and hash values for digital objects in the cloud. International Journal of Innovative Research in Computer and Communication Engineering. 2015;3.

67. Hemdan EED, Manjaiah DH. CFIM: toward building new cloud forensics investigation model. Singapore: Innovations in Electronics and Communication Engineering. Springer; 2018.

68. Liu S, et al. The research of virtual face based on deep convolutional generative adversarial networks using TensorFlow. Physica A: Statistical Mechanics and its Applications. 2019;521.

69. Povar DG, Geethakumari. A heuristic model for performing digital forensics in cloud computing environment. Berlin Heidelberg: Security in Computing and Communications. Springer; 2014.

70. Ruan K, Cloud forensics. Berlin Heidelberg: Advances in digital forensics VII. Springer; 2011.

71. Ruan K, et al. Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results. Digit Investig. 2013;10.

72. Xu Q. A novel machine learning strategy based on two-dimensional numerical models in financial engineering. Math Probl Eng. 2013;2013.

73. Xu Q, et al. Multi-feature fusion CNNs for Drosophila embryo of interest detection. Physica A: Statistical Mechanics and its Applications. 2019;531.

74. Xu Q, Li M. A new cluster computing technique for social media data analysis. Clust Comput. 2019;22.
75. Xu Q, Wu J, Chen Q. A novel mobile personalized recommended method based on money flow model for stock exchange. Math Probl Eng. 2014;2014.
76. Dawson C. Projects in computing and information systems a student ' s guide; 2005.
77. Saunders M, Lewis P, Thornhill A. Research methods for business students Fifth edition, in Research Methods for Business Students Fifth edition; 2009.
78. Lallmahomed N. Elementary statistics using JMP, J. R. Stat. Soc. Ser. A (Statistics Soc.); 2008. DOI:https://doi.org/10.1111/j.1467-985x.2008.00538_10.x
79. Sample Size Calculator.".
80. Hedberg EC, Hedberg EC. Statistical distributions. John Wiley & Sons; 2018.
81. Lehman P. 101 design methods: A structured approach for driving innovation in your organization [Book Review], no. Apr 2013. John Wiley & Sons; 2013.
82. Adams AA, McCrindle R. Pandora's box: Social and professional issues of the information age. John Wiley & Sons. 2008;1.
83. Sang T. A log-based approach to make digital forensics easier on cloud computing; 2013. DOI:https://doi.org/10.1109/ISDEA.2012.29.
84. Networks J. Securing multi-tenancy and cloud computing; 2012.
85. Passware Encryption Analyzer 2016 V.1; 2016.
86. Albaum G. The Likert scale revisited: An alternate version. Journal of the Market Research Society, 1997.
87. Approaches to the Analysis of Survey Data; 2001.
88. Dr. R. Venkitachalam, Presentation: Validity and reliability of questionnaires; 2015.
89. Ab Rahman NH, et al. Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Computing. 2016;3.
90. Alex ME, Kishore R. Forensics framework for cloud computing. Computers and Electrical Engineering. 2017;60.
91. Damshenas M, Dehghantanha A, Mahmoud R, Bin Shamsuddin S. Forensics investigation challenges in cloud computing environments; 2012. DOI:https://doi.org/10.1109/CyberSec.2012.6246092.
92. Sharma K, Kaushik PK, Agarwal PS, Jain P, Agarwal P, Dixit S. Issues and challenges of data security in a cloud computing environment. In Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). 2017;560–566.
93. Anwar U, Umair HA, Sikander A, Abedin ZU. Government cloud adoption and architecture; 2019. DOI:https://doi.org/10.1109/ICOMET.2019.8673457.
94. Baldwin J, Alhawi OMK, Shaughnessy S, Akinbi A, Dehghantanha A. Emerging from the cloud: a bibliometric analysis of cloud forensics studies. Advances in Information Security; 2018.
95. Chen L, Le-Khac NA, Schlepphorst S, Xu L. Cloud forensics, security, privacy, and digital forensics in the cloud. 2019;201–216.
96. Biggs S, Vidalis S. Cloud computing: the impact on digital forensic investigations,Conference: Internet Technology and Secured Transactions, 2009. ICITST; 2009. DOI:https://doi.org/10.1109/ICITST.2009.5402561.
97. Zafarullah, Anwar F, Anwar Z. Digital forensics for eucalyptus. in Proceedings - 2011 9th International Conference on Frontiers of Information Technology, FIT. 2011;110–116. DOI:https://doi.org/10.1109/FIT.2011.28.
98. Reilly D, Wren C, Berry T. Cloud computing: Forensic challenges for law enforcement, Internet Technol. Secur. Trans. (ICITST). 2010 Int. Conf; 2010.
99. Plunkett J, Le-Khac NA, Kechadi T. Digital forensic investigations in the cloud: A Proposed approach for irish law enforcement. 11th Annual IFIP WG 11.9 International Conference on Digital Forensics (IFIP119 2015), Orlando, Florida, United States; 2015.
100. Han J, Kim J, Lee S. 5W1H-based expression for the effective sharing of information in digital forensic investigations; arXiv Prepr. arXiv2010.15711, 2020.
101. Le-Khac L, Plunkett NA, Kechadi J, MT, Chen. Digital forensic process and model in the cloud. Security, Privacy, and Digital Forensics in the Cloud. 2019; 239.

102. Bharadiya JP, Tzenios NT, Reddy M. Forecasting of crop yield using remote sensing data, agrarian factors and machine learning approaches. Journal of Engineering Research and Reports. 2023;24(12):29-44.

103. Nallamothu PT, Bharadiya JP. Artificial intelligence in orthopedics: A concise review. Asian Journal of Orthopaedic Research. 2023;6(1):17-27.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/100348