International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

# Review on Challenges in Cloud Forensics

**Vinit Nikunjkumar Parmar[1], Dr. U. D. Rana[2], Dr. RavirajSinh Vaghela[3]**

[1]School of Cyber Security & Digital Forensics, National Forensic Sciences University Gandhinagar, Gujarat: - 382009 India
Email: *vinitparmar5329[at]gmail.com*

[2]National Forensic Sciences University Gandhinagar, Gujarat: - 382009
Email: *uttamsinh.rana[at]nfsu.ac.in*

[3]Assistant Professor at School of Cyber Security & Digital Forensics National Forensic Sciences University Gandhinagar, Gujarat: - 382009 India
Email: *ravirajsinh.vaghela[at]nfsu.ac.in*

**Abstract:** ***Cloud computing is the new term for "distributed" computing. This paradigm uses the Internet to link and communicate with IT processes, software, and hardware that are spread across several physical locations. These days, cloud computing—which facilitates data analytics in addition to storage is one of the most widely used technological components in applications. Cloud forensics can also be used to investigate insider threats and other incidents involving malicious activity by authorized users. The complicated and dynamic nature of cloud infrastructures make cloud forensics challenging. Evidence may be distributed throughout several servers and locations, making it challenging to locate and maintain. Furthermore, stringent security measures from cloud providers might make it challenging for investigators to access and review evidence. This review paper outlines the difficulties in cloud forensics and suggests a few possible solutions. This report also discusses cloud forensics' future.***

**Keywords:** Distributed, Cloud Computing, Cloud Forensics, Evidence, Investigation

## 1. Introduction

In simple terms, user can access data, application and services hosted in remote services, instead of accessing it from their computer's hard drive. Three service models, four deployment models, and five key criteria make up the NIST defined cloud model. Cloud provider, Cloud User, Cloud Agent, Cloud Accountant, and Cloud Carrier are the five attributes. Platforms as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS) are the three services. Public cloud, personal cloud, a combination of both, and shared cloud are the four deployment methods. [8] But as cloud computing becomes more common, digital forensics investigators will also confront new difficulties because evidence can now be virtualized, dispersed across several sites, and accessed through online interfaces. Moreover, investigators face unique difficulties when using virtualization technologies in cloud environments because data may be dispersed among several virtual machines.

In order to overcome these obstacles, investigators maintain chain of custody and other legal obligations while extracting and analysing data using specialised tools and methodologies. Logs and other data that can help with the inquiry may also be provided by cloud service providers. For investigators to gather, examine, and store digital evidence in cloud environments efficiently the must acquire specialized knowledge and methods.

The term "virtualization" is frequently used in reference to cloud computing. Although virtualization is a distinct technology, it is one of the most essential and fundamental elements that allows cloud computing to be flexible and scalable. Using a hypervisor, virtualization software allows you to run 1 - N virtual machines on a single physical server. This is the true benefit of virtualization software. The host's resources are dynamically distributed to the hosted virtual machines via the hypervisor as needed. (1) The market currently offers two different kinds of hypervisors.

In this research paper we will study about IOT, mobile, computer cloud related forensic challenges.

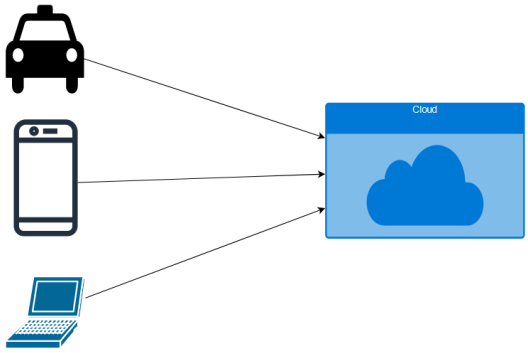
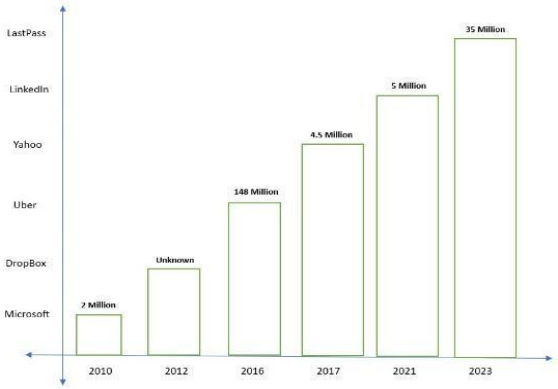



**Figure 1:** All devices connected with the Cloud

High - profile data breaches in the cloud steadily rising since 2010. Millions of accounts at companies like LinkedIn, Yahoo, and Uber have been compromised, with the trend showing no signs of slowing down. While specific numbers vary, from 2 million at Microsoft to a staggering 148 USD million at Uber, one thing remains clear: our data in the cloud is increasingly vulnerable. This underlines the urgent need for stronger cybersecurity measures, reminding us that even tech giants are not immune to the risks of cloud - based storage. It's a call to action for both enterprises and individuals to prioritize data security in this ever - evolving digital landscape.

The growing shadow of cloud data breaches demands a proactive stance. Understanding the evolving threat landscape, implementing robust mitigation strategies, and continuously researching novel attack techniques and security

measures are essential steps in this ongoing battle. Only through vigilance and innovation can we hope to secure our data in the cloud's ever - shifting landscape.




## 2. Related Work

This study explores challenges in cloud forensic investigation across identification, collection, analysis, and reporting phases. It provides recommendations to address identified difficulties based on earlier research findings [2]. This study promotes CSPs adopting a customer - centric approach, integrating advanced threat computing with hybrid cloud services for enhanced security and forensic techniques to ensure data control [3]. This study presents Secure Cloud Storage System (SCSS), employing Identity - based cryptography (IBC) with multiple PKG for enhanced key management, ensuring forensic access and outperforming comparable schemes in the literature [4].

This paper aims to identify and address cyber security issues across individuals, processes, and technologies, striving for practical, affordable, and efficient security solutions [5]. Examining security in the cloud, the paper highlights hypervisor - based technologies' role in enhancing aspects like virtual machine isolation, secure deployment, and data protection [7]. Navigating challenges and approaches in cloud forensics, the publication underscores the evolving landscape of digital forensics amid increasing reliance on cloud services [8].

Addressing virtualized system security in cloud forensics, emphasizing access restrictions, encryption, and evaluating forensic tools for investigating incidents [9]. Analysing the nexus of cloud computing architecture and digital forensics challenges, emphasizing foundational elements and their impact on data distribution in virtualized environments. [10]. Introducing a comprehensive forensic paradigm for private cloud storage, with a framework illustrated through a Sea file investigation [11].

The paper assesses cloud security risks, proposes blockchain as a solution, and introduces a novel blockchain - based forensic storage model for securing cloud data [12].

## 3. Challenges in Cloud Forensic

The many obstacles that face the several parties involved in cloud computing forensic investigation can be broadly divided into three categories: organizational, legal, and technical. These difficulties arise when duties related to identification and acquisition are inhibited, or when an examiner specializing in digital forensics is precluded from examining and interpreting data [13].

One of the most important stages of a cloud forensic investigation is the collecting phase since the data evidence must be protected from manipulation and outside influences. clarified that one of the difficulties is maintaining data integrity, which is necessary to preserve the chain of custody [2].

The distinct features of cloud computing environments present a number of difficulties for cloud forensics professionals. The dynamic nature of these settings, where data and resources are dispersed over numerous servers and regions, presents a significant difficulty. Because of this dynamic nature, it might be more difficult to identify and gather digital evidence because conventional techniques employed in on - premise settings might not be directly applicable.

The problem of multi - tenancy, in which several users share the same infrastructure, is another important obstacle. It becomes more difficult for forensic investigators to guarantee the integrity and confidentiality of evidence because of these privacy and data isolation problems.

Because encryption can make it more difficult for investigators to access and analyse data, it further complicates matters. In addition, establishing uniform and broadly applicable investigation processes is hampered by the absence of standardization in cloud forensics protocols and instruments. Notwithstanding these difficulties, continued study and development are essential to creating workable solutions that take into account how cloud forensics is changing.

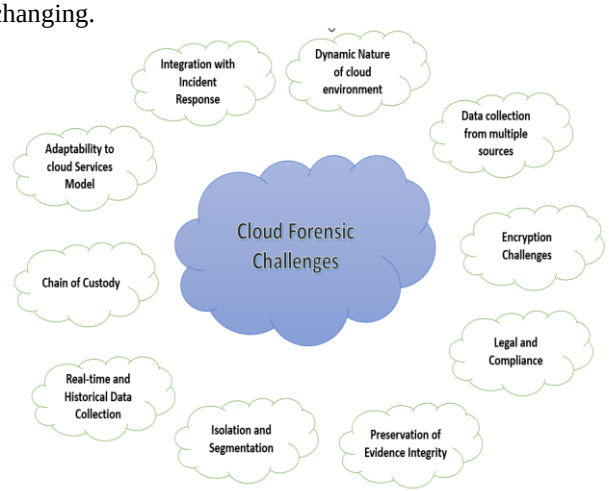



Table 1 describes the cloud forensic problems and sub - challenges. Other significant difficulties include law presentation, cross - border law, chain of custody, and crime scene reconstruction.

**Table 1:** Challenges and sub challenges in cloud forensics

| Challenges | Sub Challenges |
|---|---|
| Data Acquisition | • Physical inaccessibility<br>• Cloud Control Less<br>• Unstable Data<br>• Issues with Trust<br>• Multi - tenancy |
| Logging | • Privatization<br>• Log volatility<br>• Log accessibility |

The challenge focuses on how the "multilocation" of data stored in the cloud influences the local jurisdiction of law enforcement authorities and how this particular feature of the evidence in question impacts the law [14].

For the purpose of optimizing performance latency and data redundancy, the majority of cloud storage providers use many data servers located throughout the world. Each time a user uploads a file to the cloud, that identical file is automatically replicated and kept in two or more different physical locations—typically across different countries—at least twice (usually three times) [14].

**Table 2:** Challenges with Solutions

| No | Challenges | Comments | Recommended Solution |
|---|---|---|---|
| 1 | Cloud Dynamics | Handling the Difficulties of Quickly Changing and Provided Resources. | • Continuous Surveillance<br>• Automation<br>• Standard APIs<br>• Advanced Data Analysis |
| 2 | Data Multiplicity | Taking on the challenge of gathering and analyzing data from a variety of sources. | • Continuous Surveillance<br>• Automation<br>• Standard APIs<br>• Advanced Data Analysis |
| 3 | Encryption Challenge | Cloud forensics are complicated by encryption, which makes it difficult to access and interpret data. | • Install Endpoint Security Measures<br>• Capture Encrypted Traffic Metadata<br>• Compliance with Laws and Regulations<br>• Access Controls and Data Classification |
| 4 | Chain of Custody | In order to guarantee the integrity and admissibility of digital evidence, cloud forensics must maintain a safe and trustworthy | • Law and Compliance<br>• Service level Agreements (SLA)<br>• Hashing and Digital Signature<br>• Access Control and Permissions |
| 5 | Data Loss due to Machine Restart | Forensic investigations may face difficulties when dealing with data loss resulting from machine restarts in cloud systems. | • Use of Forensic Snapshots<br>• Incident Response Planning<br>• Secure Data Storage<br>• Documentation of Restart Events |

### 3.1 Less Control in Clouds and Dependence on the CSP

In traditional computer forensic, investigator have full control over the evidence (e. g., a hard drive confiscated by police). Figure 3 states that the limited amount of control that customers have in different layers for the three service models – IaaS, PaaS, SaaS. In IaaS, users have more control than SaaS or PaaS. The Lower level of control has made the data collection in SaaS and PaaS more challenging than in IaaS [13].

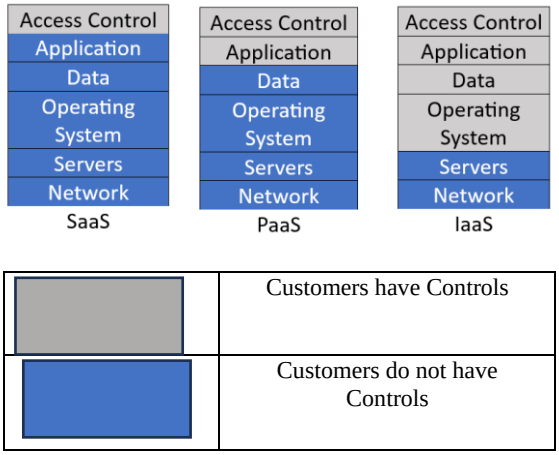



**Figure 3:** Customers' control over different layers in different service model

### 3.2 High - profile data breach cases in the cloud

**Table 3:** High - profile data breach cases in the cloud

| Year | Organization | Vulnerability | Data Loss | Financial Loss |
|---|---|---|---|---|
| 2010 | Microsoft [14] | A configuration issue within its business productivity online suite (BPOS) | Employee contact data for a small number of users were stolen. | Around USD 1 million |
| 2012 | Dropbox [15] | End users and their security settings | A total of 68 million user accounts were hacked | Unknown |
| 2016 | Uber [16] | Vulnerable Creepy Stalk version | 57 million users' data and 60 million drivers' license information were exposed | USD 148 million |
| 2017 | Yahoo [17] | Session Hijack | 3 billion user accounts hacked | USD 4.5 million |
| 2021 | LinkedIn [18] | Network Scraping | A total of 700 million user accounts posted for sale on the dark web | USD 5 million |
| 2023 | LastPass [19,20] | Targeted attack on a DevOps engineer's home computer using a vulnerability in the Plex media server package. | Obtained password vaults with encrypted and plaintext data from 25 million users. Exposed seed phrases used for cryptocurrency investments, leading to significant the | USD 35 million worth of crypto |

## 4. Tools and Technology

These tools serve various purposes in the cloud forensics investigative process, from data acquisition and analysis to network monitoring and compliance adherence.

**Table 4:** Tools and Technologies

| No | Tool | DAA | MF | NF | LA | CSPM | LA | L & C |
|---|---|---|---|---|---|---|---|---|
| 1 | EnCase Forensic | ✓ | | | | | | |
| 2 | Wireshark | | | ✓ | | | | |
| 3 | Rekall | | ✓ | | | | | |
| 4 | AWS CloudTrail | | | | | ✓ | | |
| 5 | Paraben E3: Universal | | | | | | | ✓ |
| 6 | Gray log | | | | ✓ | | | |
| 7 | SIFT Workstation | ✓ | | | | | | |
| 8 | Cloud Shark | | | ✓ | | | | |
| 9 | Palantir Gotham | | | | | | | ✓ |
| 10 | Google Cloud Audit Logs | | | | | ✓ | | |
| 11 | LiME | | ✓ | | | | | |
| 12 | ELK Stack | | | | ✓ | | | |

**DAA:** - Data Acquisition and Analysis, **MF:** - Memory Forensics, **NF:** - Network Forensics, **LA:** - Log Analysis, **CSPM:** - Cloud Service Provider Monitoring, **LA:** - Live Analysis, **L & C:** - Legal and Compliance.

***Mobile Cloud Challenges***

Mobile cloud forensics encounter difficulties with data security, heterogeneous device types, dynamic storage, network connections, and the intricate fusion of forensic methodologies throughout many mobile and cloud contexts. The indistinct boundaries separating personal and professional data on mobile devices make it more difficult for forensic investigators to make this distinction.

**Table 5:** Mobile Cloud Challenges

| Challenges | Mitigations |
|---|---|
| Data Security | Protect sensitive data in the cloud and on mobile devices by encrypting it. Put secure communication techniques into practice. Update and audit security measures on a regular basis. |
| Device Diversity | Provide forensic instruments that work on a range of mobile operating systems. Keep up with updates on new OS versions and device models. |
| Dynamic Storage Locations | Monitor alterations to the locations of data storage by implementing real-time monitoring. To collect data at several storage locations, use automated technologies. |
| Network Relational Dependencies | Use network forensic methods to examine data as it's being transmitted. Establish safe channels of communication between mobile devices and the cloud. |
| Personal and Professional Data | Provide precise guidelines for data separation. Use mobile device management (MDM) tools to keep personal and work-related data separate and safe. |

## 5. Case Study

**Table 6:** Case Study

| Affected Applications | Affected Data |
|---|---|
| 2014 Case Apple iCloud | A data breach released private celebrity images, highlighting difficulties in cloud forensics and posing issues with data ownership on third-party servers. |
| 2017 Case Amazon S3 bucket misconfiguration | cloud security issues, highlighting dangers with regard to data placement, fragmentation, and how dynamic settings affect configuration weaknesses. |
| 2012 Case Dropbox data breach | leaked 68 million users' login passwords, highlighting problems with data fragmentation and an infrastructure weakness in Dropbox. |
| 2019 Case Microsoft Office 365 data breach | caused over 300,000 consumers' personal information to be compromised by hackers gaining access to several accounts. |
| 2019 Case AWS data breach | A misconfigured firewall allowed the personal information of over 100 million customers to be taken, bringing attention to issues with cloud security and visibility. |

## 6. Future Trends

### 6.1 Cloud Forensic Learning & Development

To give people the information and abilities they need to do forensic investigations in cloud systems, cloud forensic education and training are essential. Understanding cloud computing technologies, cloud forensic frameworks, cloud forensic tools, and best practices for carrying out cloud forensic investigations should be the main topics of this program.

### 6.2 Integrating Machine Learning and AI Strategies:

The use of machine learning and artificial intelligence approaches in cloud forensics speeds up the process of finding, automatically identifying, and classifying digital evidence, hence diminishing the duration and exertion of the inquiry.

### 6.3 Establishing Integrity in Cloud Forensic Models

It is essential to develop forensic frameworks that are standardized and customized for cloud systems in light of the rapidly growing cloud computing market. These frameworks ought to provide uniform practices, guidelines, and methods that function with many cloud computing environments.

### 6.4 Collaboration and Teamwork

Strong coordination and collaboration between law enforcement agencies, cloud service providers, and forensic investigators are necessary for successful cloud forensic investigations. Forensic investigators need to work closely with cloud service providers and law enforcement agencies in order to conduct successful investigations.

### 6.5 Advances in in the cloud Forensic Software

The development of specialist tools for cloud forensics is necessary in order to retrieve, store, and examine digital evidence in cloud environments. These tools need to be specifically designed for each cloud platform and have the capacity to thoroughly evaluate data at the network, operating system, and application layers.

## 7. Discussion

In conclusion, the "Challenges in Cloud Forensics" review paper sheds light on the complexities posed by dynamic cloud environments, data multiplicity, and evidence preservation. Addressing these challenges demands proactive measures such as real - time monitoring, standardized APIs, automation, collaboration with providers, and advanced data analysis, ensuring a resilient framework for effective forensic investigations in the cloud.

The evaluation highlights how important it is to collaborate with cloud service providers, innovate continuously, and build specialized tools in order to fulfil the changing needs of cloud forensics. Understanding and overcoming these obstacles is crucial for strong cybersecurity and fruitful forensic investigations in the cloud, as enterprises use cloud technologies more and more.

## References

[1] Aalam, Zunaid, Vinod Kumar, and Surendra Gour. "A review paper on hypervisor and virtual machine security. " Journal of Physics: Conference Series. Vol.1950. No.1. IOP Publishing, 2021.
[2] Yassin, Warusia, et al. "Cloud forensic challenges and recommendations: A review. " OICCERT Journal of Cyber Security 2.1 (2020): 19 - 29.
[3] Chinedu, Paschal Uchenna, et al. "Cloud security concerns: assessing the fears of service adoption. " Archive of Science and Technology 1.2 (2020): 164 - 174.
[4] Unal, Devrim, et al. "A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity - based encryption. " Future Generation Computer Systems 125 (2021): 433 - 445.
[5] Ghaffari, Fariba, Hossein Gharaee, and Abouzar Arabsorkhi. "Cloud security issues based on people, process and technology model: a survey. " 2019 5th International Conference on web research (ICWR). IEEE, 2019.
[6] Sabahi, Farzad. "Secure virtualization for cloud environment using hypervisor - based technology. " International Journal of Machine Learning and Computing 2.1 (2012): 39.
[7] Purnaye, Prasad, and Vrushali Kulkarni. "A comprehensive study of cloud forensics. " Archives of Computational Methods in Engineering 29.1 (2022): 33 - 46.
[8] Kazim, Muhammad, and Shao Ying Zhu. "Virtualization security in cloud computing. " Guide to Security Assurance for Cloud Computing (2015): 51 - 63.
[9] Al Sadi, Ghania. "Cloud computing architecture and forensic investigation challenges. " International Journal of Computer Applications 124.7 (2015).
[10] Teing, Yee - Yang, et al. "Private cloud storage forensics: Seafile as a case study. " Handbook of Big Data and IoT Security (2019): 73 - 127.
[11] Xu, Hang, et al. "A survey: cloud data security based on blockchain technology. " 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC). IEEE, 2019.
[12] Herman, Martin, et al. Nist cloud computing forensic science challenges. US Department of Commerce, National Institute of Standards and Technology, 2020.14] Karagiannis, Christos, and Kostas Vergidis. "Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal. " Information 12.5 (2021): 181.
[13] Zawoad, Shams, and Ragib Hasan. "Cloud forensics: a meta - study of challenges, approaches, and open problems. " arXiv preprint arXiv: 1302.6312 (2013).
[14] Zuo, C.; Lin, Z.; Zhang, Y. Why does your data leak? uncovering the data leakage in cloud from mobile apps. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; IEEE: Piscataway, NJ, USA, 2019.

[15] Mondal, A.; Chatterjee, P. S. A Systematic Literature Survey on Data Security Techniques in a Cloud Environment. In Proceedings of the 2022 OITS International Conference on Information Technology (OCIT), Bhubaneswar, India, 14–16 December 2022.
[16] Chun, S. H. E - commerce liability and security breaches in mobile payment for e - business sustainability. Sustainability 2019, 11, 715. [CrossRef].
[17] Chen, D.; Chowdhury, M. M.; Latif, S. Data Breaches in Corporate Setting. In Proceedings of the 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, Mauritius, 7–8 October 2021.
[18] Jartelius, M. The 2020 Data Breach Investigations Report–a CSO's perspective. Netw. Secur.2020, 2020, 9–12
[19] Dive, C. LastPass Cyberattack Timeline.2023. Available online: https: //www.cybersecuritydive. com/news/lastpass - cyberattack - timeline/643958/ (accessed on 1 November 2023)
[20] Krebs, B. Experts Fear Crooks are Cracking Keys Stolen in LastPass Breach.2023. Available online: https: //krebsonsecurity. com/ 2023/09/experts - fear - crooks - are - cracking - keys - stolen - in - lastpass - breach/ (accessed on 1 November 2023).