Evidence Collection Complexities in Cloud Computing Platforms

Prajapati Shivam Brijraj (2405112140075)

Sharma Riya Mayur (2405112140085)

Smitkumar Pravinchandra Bariya (2405112140087)

Rinku Patil (rinku.patil31670@paruluniversity.ac.in)

MASTER OF COMPUTER APPLICATION
Parul Institute of Engineering Technology,
Vadodara, Gujarat.

***Abstract*—The advent of cloud computing has revolutionized data storage and management, concurrently giving rise to the critical field of cloud forensics, a specialized area within digital forensics. In deviation from standard digital forensics, collecting digital evidence from cloud-based platforms offers distinctive and multifaceted challenges. This analysis reviews these difficulties and explores the technical, legal, and organizational obstacles that researchers face when acquiring forensically sound data from cloud environments. Furthermore, it examines the diverse application areas where cloud forensics is of paramount importance, including criminal investigations, corporate security incidents, and legal discovery. This paper also outlines the methodologies, algorithms, techniques, and tools currently employed and under development to resolve the challenges of collecting digital evidence from cloud-based platforms. Finally, it highlights the ongoing research and development efforts influencing the trajectory of this essential discipline, aiming to deliver an exhaustive insight into the evolving landscape of cloud forensics**

Keywords— cloud forensics, digital evidence, data volatility, jurisdiction, encryption, multi-tenancy

Hypothesis

"Adaptive forensic tools (e.g., AI-powered log correlation, blockchain-based evidence tracking) combined with coordinated international legal frameworks will significantly mitigate cloud forensic challenges, enabling efficient cross-border investigations."

I. Introduction

Cloud computing represents a revolutionary technology that delivers computing services, surround applications, databases, networking, and servers, typically on a pay-per-use basis.1 This model shift in how organizations and individuals store and manage data has led to the emergence of cloud forensics, a specialized branch of digital forensics that focuses on investigating data distributed across cloud environments. As cloud computing becomes increasingly ubiquitous, the necessity for effective cloud forensics capabilities has grown exponentially.1 The ability to carry out in-depth evaluations in the cloud is essential for addressing security incidents, cybercrimes, and legal matters in this evolving digital environment 5

To perform cloud forensics, one needs to have a good understanding of cloud service models (SaaS, PaaS, and IaaS) and service delivery types (such as public, private, hybrid, and community clouds). How to gather digital evidence and the issues it brings along depend largely on the model at stake. Unlike classic, which is generally digital forensics based on direct access to physical devices, when the forensic investigation is carried out in a cloud environment is limited by several different issues. These factors include the lack of physical control over the hardware itself, geographically spread and normally cross-jurisdictional data, and reliance on Cloud Service Providers (CSPs) to retrieve evidence. These differences also increase the demand for customized forensic models and dedicated tools to analyze the artifacts of cloud architecture. Therefore, this study focuses on a detailed analysis of these challenges and provides a survey of the approaches used for the acquisition of evidence in cloud ecosystems..

II. Challenges in Collecting Digital Evidence from Cloud-Based Platforms

The process of gathering digital evidence in cloud-based environments is more complex than that in traditional systems. Investigators must deal with a combination of technical limitations, legal restrictions, and organizational barriers, all of which make cloud forensics a uniquely challenging field of study.

A. ***Technical Challenges***

An important difficulty in cloud forensics is that there is no direct physical access to the hardware components. As servers and their peripherals are all physically maintained by cloud service providers (CSPs), it is up to them to provide available evidence to investigators. This dependency can lead to delays, reduced visibility, and barriers set by the CSP's internal policy and technical constraints. Unlike a forensic examination, in which examiners have direct control of the evidence they are examining and can maintain its security, a cloud environment may impose a dependence relationship on the examiner, making the acquisition and authentication processes more difficult. Owing to the ever-changing characteristics of the cloud environment, maintaining data integrity and handling volatility issues is challenging. As cloud data stores are constantly updated, reused, replaced, and deleted quickly, the information cannot remain the same.

It can be extremely challenging for forensic investigators to seize and maintain fugacious artifacts, such as memory data, network packets captured in real time, or cached data from web browsing. Cloud vendors usually distribute data between multiple servers at different locations to provide better performance. While this strategy ensures an efficient distribution of the body of evidence, it brings considerable

difficulty during video evidence reconstruction and retracing, back to its source. Therefore, data collected from clouds is usually volatile and scattered over a large area, and temporal and special acquisition methods are necessary to ensure the data are reliable and authentic.

It's an integral aspect of the public cloud, with shared computing power among many customers simultaneously. While this has made it very efficient, it has also created numerous forensic problems. Investigators must work carefully to isolate one tenant's digital evidence from other tenants' data, while continuing to provide service. Therefore, forensic-based methodologies are needed not only to precisely detect the valuable data, but also to ensure privacy and minimal intrusion to other users.

To ensure the confidentiality and integrity of user data, data encryption is commonly employed by Cloud Service Providers (CSPs). While the implementation of encryption is essential for the protection of privacy, it raises some challenges for the digital forensic domain, where direct access to the data is not feasible. Usually, investigators depend on decryption keys to move forward, and they are very difficult to come by (legally).

Another major challenge is log management on cloud platforms. Logs are typically scattered across layers of the infrastructure, so they are both decentralized and potentially unreliable. Retention and archival policies of log events may vary greatly among cloud service providers (CSPs), as does the availability of historical log records. Even if logs are available, there is no assurance that they are uniform, include all the required data, etc., which makes the forensic investigation onerous.

B. Legal and Jurisdictional Challenges

Cloud storage services commonly distribute data between server farms in various regions around the world, producing difficult, legal, and geographical challenges for investigators. And when the police want digital evidence that could lead to an arrest, they may have to abide by laws in more than one country if the data is stored outside of their jurisdiction. The investigation is made more difficult by restrictions in cross-border access to data sets and in differing interpretations of privacy or security laws in different locations.

Figuring out who can access data stored in the cloud remains a challenge, with law enforcement tied to annoyingly strict policies (directives like the GDPR in Europe or the Cope in California) standing in the way. To legally obtain the digital evidence, the correct order needs to be in place, and detectives need to consider the varying privacy standards in the various jurisdictions. This creates a modern-day ethical conundrum, which is the balance between continuing to search for evidence and protecting the rights of the individual. In addition, leases and service contracts provided by cloud service providers (CPSs) could impact forensic data accessibility, and therefore what can be recovered. As a result, knowing what the elements and outcomes of the contractual negotiation you are negotiating are is crucial in order to remain in compliance with the law for the duration of the forensic investigation.

C. Organizational and Procedural Challenges

The Lack of standard policies and procedures among CSPs is one of the challenges in cloud forensics. Given that each provider has its own security policies, investigators are often challenged to administer a consistent process for collecting and analyzing digital evidence. Without standardized practices, forensic analysis is not the same at each organization, which creates increased levels of complexity and higher costs for entities that are conducting the examination.

By contrast, cloud forensics is a different skillset beyond conventional digital forensics (DF). With the rapid development of cloud technologies, investigators are required to continuously learn and improve their skills to remain relevant in their fields. A further challenge is to maintain a forensically sound chain of custody because evidence in cloud systems is distributed and virtualized. To preserve the validity and relevance of the information recorded, investigators are expected to document each interaction carefully and by universal standards during the investigation process.

III. APPLICATION AREA OF CLOUD FORENSICS

Cloud forensics is becoming relevant in numerous practical scenarios, largely because organizations in different industries are now heavily dependent on cloud services. As this dependence grows, the need for effective forensic techniques to investigate and secure cloud environments continues to increase.

A. Criminal Investigations

Cloud forensics is an essential aspect of the modern cybercrime investigation process. It also allows police access to investigate crimes that occur on the internet or via computer, such as online fraud, or when suspects are believed to be using cloud services to communicate or store evidence of their involvement in crime, like sharing terrorist or other illegal material. By harvesting and analyzing cyber footprints stored in the cloud (file repositories, e-mail systems, collaborative environments), investigators are able to zoom in on suspects and create credible evidence for further prosecution. A record of key SATCOM investigations. Successful investigation and analysis of cloud-based evidence is often the linchpin to reaching a resolution of a Digital Crime.

B. Corporate Security Incidents

In corporate security terms, cloud forensics is critical for handling incidents of data breaches, insider threats, and organizational policy violations. Upon breach, forensic methods allow investigators to measure the extent of the compromise, the paths used to perform the attack, and the individuals responsible for certain actions. In addition to reactive processes, cloud forensics also participates in recovery by reducing destruction, recovering affected systems, and attempting to restore lost data. More importantly, it can be used proactively to help enterprises identify the vulnerabilities of their cloud infrastructure and analyze user behavior to identify any exploitation from within and strengthen their overall security fabric.

C. Legal Discovery (e-Discovery)

Cloud forensics plays a vital role in the realm of legal discovery (e-discovery) 8): the process of finding, preserving, gathering, and presenting electronically stored information (ESI) as evidence for use in legal proceedings. As a significant percentage of organizational data has been migrated to cloud repositories, attorneys must be able to access and review information contained within cloud-based

services (e.g., email systems, shared document repositories, and collaborative services). E-discovery and e-forensics both deal with electronic data but have different purposes and run under different legal and procedural guidelines. Cloud forensics helps investigators to properly gather digital evidence from a cloud environment that is forensically sound and acceptable in court for litigation, regulatory needs, and internal investigations.

IV. Methodologies and Frameworks for Cloud Forensic Investigation

Cloud forensic investigations generally follow the established phases of digital forensics, which are adapted to the specific challenges of cloud environments. Digital investigators follow a sequence of phases in the investigation, starting with identifying the incident and potential evidence sources, and then preserving the integrity of the data.

This analysis is possible by collecting digital traces, analyzing and examining them, and then reporting the findings in the final report. When it comes to cloud, we need to modify the above approach according to the service model we are using. Software as a Service (SaaS) or Cloud. As noted earlier, investigators commonly depend on APIs from providers to extract user data, activity logs, and other information from them. PAAS cases typically need a focus on application-level logs and data available through development tools. As a counterexample, Infrastructure as a Service (IaaS) may allow users to purchase a virtual machine image and traces of network traffic. In addition, low-level system logs can be accessed depending on the contractual agreements with the CSP.

These models are designed mainly to offer standard procedures to support investigators in effectively handling challenges in cloud environments, while carrying out a thorough and legally sound investigation.

Furthermore, legal considerations determine cloud forensic procedures to a large extent. Risks associated with jurisdictional conflicts and regional and multinational laws on data protection, and the requirement that legal approvals (warrants, user consent, etc.) be obtained before processing evidence from cloud platforms.

V. Algorithms and Technical Techniques Employed in Cloud Forensics

Algorithms and specialized methods are vital for collecting and analyzing digital evidence from cloud environments. These ensure that investigators can extract information accurately and maintain data integrity during the examination.

- ***Data Carving***

In cloud environments, specialized systems are commonly employed to collect and examine extensive log data generated by a wide range of resources.

- ***Network Forensics in Cloud Environments***

Formalities are cloud-oriented in that they work in a cloudy environment for capturing and monitoring network packets for finding evidence of wrong action or data spillage. 6 This may include network packet capture, analyzing traffic patterns to find abnormal selectivity in message sending, or examining flow records to identify communication between hosts. 6 Cloud is a virtualized network, and the use of traditional network monitoring tools may require tweaks or the use of cloud-native network monitoring tools to provide visibility of network traffic.

A. ***Tools and Technologies for Cloud Forensics***

A variety of tools and technologies are available to assist in the collection, analysis, and preservation of digital evidence from the cloud

- ***Open-Source Tool***

Most cloud forensics tasks leverage popular open-source solutions. 8 The Sleuth Kit (TSK) The Sleuth Kit (TSK) and its user interface, Autopsy, are valuable tools for the analysis of disk images and file recovery. 8 Volatility is a popular repository for analyzing RAM dumps. 8 OSQuery enables database-like access to OS data for analyzing cloud instances. 105 There are cloud-specific open-source tools such as Google Cloud Forensics Utils, which offers tools for incident forensics on the Google Cloud Platform. 19 These may have a high degree of flexibility, and in principle, they are open-source tools that can be adapted to obtain what is required of them during the investigation..

- ***Commercial Tools***

Many commercial forensic suites and toolsets have powerful capabilities for conducting cloud forensics. 7 Oxygen Forensic Detective is the all-in-one forensic tool that allows you to extract and analyze user data from a variety of sources: 10 Magnet AXIOM is a reliable application for providing digital evidence from mobile, computer and cloud sources. 10 FTK and EnCase tools are well known in law enforcement agencies and enterprises for digital forensics, including cloud forensics. Both allow for deep inspection. 119; also, cloud-native security vendors, including Wiz and Cado Security, are entering the space, providing natively integrated cloud forensics solutions which automatically collect and analyse data across multi-cloud environments

- ***Cloud Provider Native Tool***

All major cloud providers also provide a rich set of native services to help people perform cloud forensics within these frameworks. 8 AWS CloudTrail logs API calls to AWS services to provide a history of the activity. 6 AWS CloudWatch monitors applications and resources by generating logs and metrics. 6 Azure Monitor provides equivalent logging and monitoring features for the Azure resources. 8 GCP Cloud Audit Logs monitor administrative and user access to the GCP. 28 These are general tools that are usually the easiest to use when investigating security incidents in a given cloud environment.

VI. Current and Latest Research and Development in Cloud Forensics

Cloud forensics has been developing rapidly in response to the ongoing challenges and benefits of new technologies. 3 Recent advances have concentrated on finding better solutions dealing with issues of data volatility and impar behavior on cloud resources. 3There is also ongoing work to develop methods for both live forensics and anti-forensics for volatile evidence capture. 6

Jurisdictional complexities remain a specific focus. 3 Researchers are examining legal systems and international cooperation as a means to better collect evidence across borders. 1

The use of new technologies such as AI, ML, and blockchain is also being experimented with in cloud forensics. 3 Various

AI and ML algorithms have been developed to improve data analysis, pinpoint exceptions, and streamline investigations. 33 Exploring Blockchain technology for authenticating and preserving digital evidence acquired from the cloud. 3 They want to develop a more effective, precise, and legally admissible approach for cloud forensic investigations.

VII.CONCLUSION

The acquisition of digital evidence hosted in the cloud is challenging due to many evolving technical, legal, and organizational issues. The nature of cloud computing - a model lacking physical access, data transiency, multi-tenancy, and global sparsity - requires forensic methodologies, processes, procedures, and technology. With increasing cloud adoption in different domains, the significance of good cloud forensics cannot be exaggerated. It is an important tool in the fields of criminal investigation, corporate security, and legal discovery, where the emphasis is on the ability to collect, analyze, process, and preserve digital evidence in such a way that it remains forensically sound in the form of a standard digital format and can be presented in a court of law. Current research is being conducted to address these limitations, and new technologies such as AI, machine learning, big data, and blockchain have been exploited to improve cloud forensics. The future of such a will most likely have a higher degree of automation, standardization, and sweeter tools and uniform structures to lead our way through the woods and light at the end of the cloud tunnel for a better a safer digital world.

TABLE I.

COMPARISON OF CLOUD SERVICE MODELS AND THEIR FORENSIC IMPLICATIONS

Service Model	Description / Typical Data Sources	Key Forensic Challenges	Common Acquisition Methods
SaaS	Software is delivered via the web. The app saves logs, data, and user activity.	Limited access to the underlying infrastructure, dependency on the provider's logging and retention policies.	Vendor API, exporting of user-level data.
PaaS	Platform as a service for application development, execution, and management. Application, middleware, developer activity, OS, and container logs.	Responsibilities of the Shared Model, complexity in getting to infrastructure. .	Access to platform services via API, CLI tools, and perhaps container file system access.
IaaS	Provides compute, storage, and networking. Virtual machine, hypervisor, network traffic, storage, and memory dump logs.	These are instability of the virtual machines, distributed storage, and inability to directly access the hardware	VM capture, storage capture, network capture, memory acquisition tools, and forensic VMs.

TABLE II.

Taxonomy of Cloud Forensics Data Collection Challenges

High-Level Category	Specific Challenge	Description
CSP Related Challenges	Need to rely on Cloud Service Provider	Direct control is not available to the entities such as the ISPs; and there is delay and lack of coverage by CSPs also.
CSP Related Challenges	Virtualization of data storage	Data stored on shared physical devices makes isolation of specific user data difficult.
Storage & Accessibility Challenges	impermanence of data	Temporary files like registry entries and internet files are deleted after a set time, hindering collection.
Storage & Accessibility Challenges	Volume of Data	Traditional forensic tools are unable to cope with huge amounts of cloud data, the tools used for cloud service evidence collection are more specialized
Storage & Accessibility Challenges	Decentralized Data	Data distributed across multiple centers and geographies complicates complete evidence collection.
Other Challenges	Multi-tenancy	Shared infrastructure makes segregating forensic data while maintaining privacy complex.

Other Challenges	Data Volatility	Cloud data may be readily modified or deleted and can impact the integrity and accessibility of evidence.

TABLE III.

Overview of Popular Cloud Forensics Tools

Tool Name	Type	Key Features Relevant to Cloud Forensics	Provider / Developer
The Sleuth Kit (TSK)	Open-Source	Analysis of disk image, analysis of file system, Data Carving.	Sleuth Kit Labs
Autopsy	Open-Source	GUI based, compatible with TSK, timeline and keyword searching capabilities.	Basis Technology
Volatility	Open-Source	Forensics framework for RAM dumping on Windows based systems.	Volatility Foundation
Oxygen Forensic Detective	Commercial	All-In-One, Computer & Cloud, Mobile & Computer Forensics.	Oxygen Forensics
Magnet AXIOM	Commercial	Mandiant Mobile, Cloud, and Computer Acquisition & Analysis With advanced analytics.	Magnet Forensics
FTK (Forensic Toolkit)	Commercial	Full-disk image collection, analysis, and supports cloud data.	Exterro
EnCase	Commercial	Set of tools for digital forensic, system analysis, and incident response.	OpenText
Google Cloud Forensics Utils	Open-Source	A set of related tools for common incident investigation on Google Cloud.	Google
AWS Audit Manager	Cloud Provider Native	Automates evidence collection for compliance.	Amazon Web Services
Azure Monitor	Cloud Provider Native	Logging and monitoring for forensic analysis.	Microsoft Azure
GCP Cloud Audit Logs	Cloud Provider Native	Tracks administrative and data access.	Google Cloud Platform

VII. BIBLIOGRAPHY / REFERENCES

1. A list of relevant academic papers, technical reports, and other credible sources encountered during the research process would be compiled here, following a consistent citation style, to provide a comprehensive record of the materials that informed this report.

1. Challenges of Investigations in the Cloud – Cyber - University of Hawaii West Oahu, accessed April 29, 2025, https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/challenges-of-investigations-in-the-cloud/

3. Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics - DigitalCommons@UNO, accessed April 29, 2025, https://digitalcommons.unomaha.edu/cgi/viewcontent.cgi?article=1043&context=interdiscipinformaticsfacpub

4. Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review - MDPI, accessed April 29, 2025, https://www.mdpi.com/2073-431X/13/8/213

5. Digital Evidence Data Collection: Cloud Challenges - IEEE Computer Society, accessed April 29, 2025, https://www.computer.org/csdl/proceedings-article/big-data/2021/09672014/1A8hsnt94fC

6. Digital Forensic Investigation Standards in Cloud Computing - Scientific Publications, accessed April 29, 2025, https://www.scipublications.com/journal/index.php/ujcsc/arti

cle/view/923
7. Uncovering Digital Evidence: Navigating the Complexities of Cloud Computing Forensic Science - Cheap SSL Certificates, accessed April 29, 2025, https://www.ssl2buy.com/cybersecurity/cloud-computing-forensic-science
8. What is Cloud Forensics? - CrowdStrike, accessed April 29, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-forensics/
9. What Is Cloud Forensics? - Wiz, accessed April 29, 2025, https://www.wiz.io/academy/cloud-forensics
10. Cloud Digital Forensics - Aqua Security, accessed April 29, 2025, https://www.aquasec.com/cloud-native-academy/cspm/cloud-digital-forensics/
11. Cloud Forensics - History, Types, and Benefits, accessed April 29, 2025, https://www.oxygenforensics.com/en/resources/cloud-forensics/