GAS Journal of Engineering and Technology (GASJET)

Volume 3 | Issue 3, 2026 Homepage: https://gaspublishers.com/gasjet-home/ ISSN: 3048-5800

Cloud Forensic Tools and Storage: A Systematic Mapping Study

Frank Idugboe[1], Warley Junior[2], and Vitor Castro[3]

[1,2,3]Department of Forensic Science, Universidade Federal do Sul e Sudeste do Pará, Marabá, Brazil

Received: *10.03.2026* | ***Accepted:*** *27.03.2026* | ***Published:*** *29.03.2026*

***Corresponding Author:** Frank Idugboe

DOI: *10.5281/zenodo.19313810*

Abstract **Original Research Article**

Cloud computing has fundamentally transformed digital forensic investigations by introducing distributed, multi-tenant, and highly dynamic environments where traditional acquisition methods are no longer feasible. The rapid evolution of cloud service models, including IaaS, PaaS, and SaaS, alongside containerised and microservice architectures, has resulted in a fragmented landscape of forensic tools and approaches. This study presents a systematic mapping of cloud forensic tools and storage-related techniques published between 2020 and 2025. Using a structured methodology applied to IEEE Xplore, ACM Digital Library, and ScienceDirect, 12 primary studies were selected from an initial pool of 120 records. These studies were classified according to service models, forensic phases, storage artifacts, and technical challenges. The results show a shift toward log-centric and metadata-driven investigations, particularly in SaaS environments, while traditional disk-based analysis remains limited to IaaS contexts. Emerging areas such as container and ephemeral storage forensics remain underdeveloped. Three major challenges are identified: evidence volatility, data scale, and trust in provider-controlled infrastructures. Although solutions such as automated analysis and Zero Trust models exist, most remain at early stages. The findings highlight the need for cloud-native, scalable, and transparent forensic frameworks to support reliable and legally defensible investigations.

Keywords: Cloud forensics, digital forensics, cloud computing, log analysis, container forensics, Zero Trust.

1. INTRODUCTION

The rapid adoption of cloud computing has fundamentally transformed how organisations deploy, manage, and store digital resources. While this transformation has enabled scalability, flexibility, and cost efficiency, it has also introduced significant challenges for digital forensic investigations. Traditional forensic methodologies were developed for environments where investigators had physical access to hardware, enabling the seizure of storage devices, creation of forensic images, and controlled laboratory analysis. In contrast, cloud environments are characterised by distributed storage, virtualised infrastructure, multi-tenancy, and remote access through provider-controlled interfaces, which significantly complicate evidence acquisition, preservation, and validation [1], [2]. To address these challenges, cloud forensics has emerged as a specialised domain that focuses on the identification, collection, preservation, and analysis of digital evidence in cloud environments. Unlike conventional forensic investigations, cloud forensic processes rely primarily on logical acquisition techniques, including virtual machine snapshots, audit logs, metadata, and API-based data retrieval, rather than direct physical access to storage media. This shift fundamentally alters both the nature of

available evidence and the methods required to ensure its integrity and legal admissibility.

The complexity of cloud forensic investigations is further amplified by the diversity of cloud service models. In Infrastructure-as-a-Service (IaaS), investigators may retain partial access to virtual machines and storage volumes, allowing limited application of traditional techniques. However, in Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) environments, abstraction layers restrict visibility, forcing investigators to rely predominantly on logs, application data, and provider-generated metadata. Recent developments in containerisation and microservice architectures, particularly through platforms such as Docker and Kubernetes, have introduced highly dynamic and ephemeral environments in which workloads and associated storage artifacts may exist only for short durations [3]. This creates a "race to acquisition," where relevant evidence must be captured before it is automatically removed or overwritten.

In parallel, evolving security paradigms such as Zero Trust have challenged traditional assumptions about trusted infrastructure. Conventional forensic approaches often assume that hypervisors, cloud management planes, and privileged administrators can be relied upon to provide accurate and untampered evidence. However, Zero Trust models reject implicit trust and emphasise continuous verification, raising critical concerns about how evidence integrity can be maintained in potentially untrusted environments [4]. At the same time, modern cloud systems generate vast volumes of logs and activity data, making manual analysis impractical. As a result, there is increasing reliance on automated and data-driven forensic techniques. While these approaches improve scalability, they introduce new challenges related to transparency, explainability, and legal defensibility, particularly when forensic findings must be presented in court [5]. Despite the growing body of research in cloud forensics, several critical gaps remain. First, there is an authenticity gap in Zero Trust environments, where existing tools often assume trusted infrastructure and lack mechanisms for independently verifiable evidence collection [4]. Second, there is a transparency gap associated with automated forensic analysis, as many data-driven approaches do not provide the level of explainability and auditability required for legal validation [5]. Third, there is a volatility gap related to containerised and serverless environments, where traditional tools designed for persistent storage are insufficient to capture short-lived artifacts effectively. Furthermore, existing surveys tend to focus either on legal and regulatory aspects or provide high-level overviews of tools, without systematically linking forensic techniques to specific storage artifacts and cloud service models [6].

To address these limitations, this study conducts a systematic mapping of cloud forensic tools and storage-related investigation techniques published between 2020 and 2025. Unlike existing reviews, this work explicitly links forensic tools to cloud service models, forensic process phases, and storage artifacts, enabling a more fine-grained analysis of technical capabilities and limitations. The objective is to provide a structured understanding of how current approaches operate within modern cloud environments and to identify gaps that hinder practical adoption.

This study makes three main contributions. First, it provides a structured classification of cloud forensic research across service models, forensic phases, and storage artifacts. Second, it identifies and analyses key technical challenges, including volatility, scalability, and trust, and maps them to existing solution approaches. Third, it highlights critical research gaps, particularly in container forensics, forensic readiness, and transparent automated analysis, thereby offering a foundation for future research.

By systematically analysing recent literature, this study aims to support both researchers and practitioners in understanding the current state of cloud forensic tools and in developing more robust, scalable, and legally defensible investigation frameworks.

2. Related Literature

2.1 Foundational Challenges in Cloud Forensics

Cloud forensics was established to address the fundamental mismatch between traditional forensic practices and the characteristics of cloud computing

environments. Early definitions emphasised the loss of physical control, the distributed nature of storage, and the dependency on service providers for evidence acquisition [2]. These characteristics continue to shape the field, particularly by constraining the types of artifacts available to investigators and influencing the reliability of collected evidence. The NIST cloud forensic science report remains one of the most comprehensive references, identifying a wide range of challenges including data access limitations, multi-tenancy issues, and jurisdictional complexity [1]. Among these, reduced access to forensic data is consistently recognised as the most critical issue, as investigators must rely on logical acquisition via provider interfaces rather than direct disk imaging. However, while NIST provides a broad taxonomy of challenges, it does not evaluate how contemporary tools operationalise these concepts, especially in environments shaped by containerisation and microservices. Consequently, a gap persists between high-level problem identification and practical tool-oriented solutions.

2.2 Trust and Evidence Integrity under Zero Trust Assumptions

The issue of trust has become increasingly central in cloud forensic research. Traditional forensic workflows implicitly assume that infrastructure components, such as hypervisors and cloud management planes, are trustworthy sources of evidence. This assumption is increasingly challenged by Zero Trust security models, which advocate continuous verification rather than implicit trust. Scanlon et al. highlight the need to reconsider trust assumptions in digital investigations, arguing that reliance on provider-controlled infrastructure introduces potential vulnerabilities in evidence integrity [10]. Extending this argument, Tyagi et al. propose a Zero Trust-based forensic model that incorporates cryptographic validation and tamper-evident chains of custody to ensure the reliability of collected evidence [4]. These approaches represent a conceptual shift from static acquisition toward continuous and verifiable forensic readiness. Despite their theoretical strength, these models remain largely conceptual or experimental. There is limited empirical validation demonstrating their scalability or integration with existing forensic workflows. Moreover, few studies address the practical trade-offs between security, performance, and usability when implementing Zero Trust forensic mechanisms. This indicates that, while the authenticity problem is well recognised, it is not yet fully resolved in operational settings.

2.3 Automated Analysis and the Transparency Problem

The increasing volume of cloud-generated data has driven significant interest in automated forensic analysis techniques. Logs, activity records, and metadata streams generated by cloud services are often too large and complex for manual analysis, necessitating the use of data-driven approaches. Yao et al. provide a comprehensive review of automated techniques, including machine learning and large-scale data processing methods applied to cybersecurity and forensic tasks [5]. These techniques enable efficient filtering, correlation, and anomaly detection, making them well-suited for cloud environments characterised by high data velocity and volume. Similarly, recent studies on automated log analysis demonstrate improvements in investigation speed and scalability. However, a critical limitation emerges across this body of work: the lack of transparency and explainability. Many automated systems operate as opaque processes, producing results without clear reasoning paths. In forensic contexts, this creates a significant challenge, as evidence must be explainable and defensible in legal proceedings. While some studies acknowledge this issue, few provide concrete solutions for integrating interpretability into automated forensic workflows. As a result, there is a persistent tension between analytical efficiency and evidentiary reliability that remains insufficiently addressed.

2.4 Forensics in Containerised and Cloud-Native Environments

The transition toward cloud-native architectures, particularly those based on containers and microservices, has introduced new complexities for forensic investigation. Unlike traditional virtual machines, containers are lightweight, highly

dynamic, and often short-lived, making evidence collection more time-sensitive and technically challenging. Franco et al. demonstrate how container-based environments complicate forensic analysis due to the volatility of runtime artifacts and distributed logging mechanisms [12]. Elie et al. further extend this work by proposing automated acquisition techniques for container-as-a-service environments, aiming to capture container volumes and logs before they are lost [13]. These studies highlight the need for specialised tools capable of operating within orchestration platforms such as Kubernetes. However, compared to research on log analysis and traditional cloud environments, container forensics remains underdeveloped. Existing approaches are often limited to specific platforms or experimental setups, and there is a lack of standardised methodologies for preserving ephemeral artifacts. This suggests that current forensic tools have not yet fully adapted to the realities of modern cloud-native systems, reinforcing the volatility gap identified in this study.

2.5 Broader Cloud and Edge Forensic Challenges

Beyond specific tools and techniques, several studies examine systemic challenges in cloud and edge computing environments. Kebande et al. identify issues such as data heterogeneity, distributed evidence sources, scalability, and cross-layer correlation as major obstacles to effective forensic investigation [9]. These challenges are particularly pronounced in hybrid and multi-cloud environments, where evidence may span multiple providers and jurisdictions. While these studies provide valuable conceptual frameworks, they often lack detailed analysis of how specific tools address these challenges in practice. In particular, there is limited work on integrating evidence across service layers and providers in a coherent and automated manner. This highlights a gap between high-level architectural challenges and tool-level implementations.

2.6 Application-Specific Forensic Approaches

A number of studies focus on specialised forensic scenarios within cloud environments. For instance, Al-rimy et al. investigate ransomware-related forensic techniques, emphasising the analysis of encrypted files and behavioral indicators [11]. Similarly, Gulyamov et al. explore metadata extraction techniques, demonstrating how indirect artifacts can support evidentiary reconstruction [14]. While these studies contribute valuable domain-specific insights, they are typically limited in scope and do not generalise across different cloud service models or forensic processes. As a result, their contributions are best understood as complementary to broader forensic frameworks rather than as comprehensive solutions.

2.7 Synthesis and Research Gap

The reviewed literature demonstrates that cloud forensics is an active and evolving field, with significant contributions in areas such as automated analysis, Zero Trust models, and container-based investigation. However, the research remains fragmented, with limited integration across different dimensions of the problem. Three key gaps emerge from this synthesis. First, there is a lack of practical and scalable solutions for ensuring evidence authenticity in Zero Trust environments. Second, automated forensic techniques, while effective for large-scale analysis, often lack transparency and explainability required for legal validation. Third, support for volatile and ephemeral artifacts in containerised systems remains insufficient, reflecting a lag between technological evolution and forensic tool development. Furthermore, existing reviews tend to focus either on legal considerations or on high-level conceptual challenges, without systematically linking forensic tools to specific service models, storage artifacts, and process phases. This lack of structured mapping limits the ability to assess the maturity of current solutions and to identify concrete areas for improvement. To address these limitations, this study provides a systematic mapping of cloud forensic tools, explicitly analysing how they relate to storage artifacts, service models, and forensic processes. By doing so, it offers a more integrated and technically grounded understanding of the current research landscape.

3. Materials and Methods

3.1 Study Design and Planning

This study adopts a Systematic Mapping Study (SMS) approach to provide a structured overview of research on cloud forensic tools and storage-related investigation techniques. The methodology follows the guidelines proposed by Petersen et al. [7], which emphasise systematic identification, classification, and analysis of research contributions. Unlike systematic literature reviews that aim to answer narrowly defined research questions, the SMS approach is designed to map the breadth of a research field and identify trends, clusters, and gaps. The study was guided by predefined research questions focusing on cloud service models, forensic process phases, storage artifacts, and technical challenges. These dimensions were selected to capture both the technological and procedural aspects of cloud forensic investigations. The planning phase also involved defining the search strategy, selection criteria, and data extraction framework to ensure consistency and reproducibility throughout the study.

3.2 Search Strategy

The search strategy was designed to capture studies at the intersection of cloud computing, digital forensics, and storage-related tools or artifacts. A Boolean search string was constructed to combine these key concepts, ensuring broad coverage while maintaining relevance. The search string included terms related to cloud service models, forensic investigation processes, and storage artifacts such as logs and snapshots. The query was applied to three major academic databases: IEEE Xplore, ACM Digital Library, and ScienceDirect. These databases were selected because they provide comprehensive coverage of peer-reviewed research in computing, cybersecurity, and digital forensics. The search was conducted in August 2025, ensuring that recent developments in cloud-native and container-based environments were included in the study.

3.3 Study Selection Process

The study selection process followed a structured multi-stage procedure inspired by PRISMA principles for systematic reviews. Initially, the search returned 120 unique records across the selected databases. In the first stage, titles and abstracts were screened to remove studies that were clearly unrelated to cloud forensics or lacked a technical focus. This screening resulted in the exclusion of 74 records. In the second stage, the remaining studies were subjected to full-text review to assess their eligibility based on predefined criteria. During this phase, 34 additional studies were excluded due to insufficient relevance, lack of technical contribution, or failure to address storage-related forensic artifacts. The final dataset consisted of 12 primary studies, which were selected for detailed analysis. This structured selection process ensures transparency and reduces the likelihood of selection bias by applying consistent criteria at each stage of filtering.

3.4 Inclusion and Exclusion Criteria

To ensure the relevance and quality of the selected studies, explicit inclusion and exclusion criteria were defined prior to the screening process. Studies were included if they proposed, developed, evaluated, or analysed tools or techniques relevant to cloud forensics and explicitly addressed storage-related artifacts such as logs, disk images, snapshots, memory, or metadata. Only full-length papers published in English between January 2020 and December 2025 were considered. Preference was given to peer-reviewed journal articles and high-quality conference publications with clearly described methodologies. Studies were excluded if they focused solely on legal, organisational, or policy issues without providing a substantive technical contribution. Short publications such as abstracts, posters, and editorials were also excluded, as were duplicate records identified across the selected databases. These criteria were designed to ensure that the final set of studies provided meaningful insights into technical aspects of cloud forensic tools and storage analysis.

3.5 Data Extraction

Data extraction was conducted systematically using a predefined framework to ensure consistency across studies. For each selected paper, key information was recorded, including bibliographic details, research objectives, contribution type, target cloud

environment, and the specific forensic problem addressed. Additional information was extracted regarding the storage artifacts analysed, the forensic process phase targeted, and the technical challenges and solutions proposed. Each study was assigned a unique identifier, labelled P1 to P12, to facilitate referencing during analysis and discussion. This structured extraction process enabled comparative analysis across studies and supported the development of the classification scheme used in this mapping.

3.6 Classification and Coding Scheme

To address the research questions, the selected studies were classified along multiple dimensions reflecting key aspects of cloud forensic investigation. First, each study was categorised according to the cloud service model it primarily addressed, including IaaS, PaaS, SaaS, or a generic classification when the approach applied across multiple models. This classification supports the analysis of how forensic tools align with different levels of cloud abstraction. Second, studies were mapped to the phase of the digital forensic process they emphasised. The classification included acquisition, analysis, preservation, readiness, and review, allowing the study to identify which stages of the forensic lifecycle receive the most attention in current research. Third, the studies were categorised based on the types of storage artifacts they targeted. These included logs, disk and snapshot data, memory, metadata, and container or ephemeral storage. This dimension is particularly important for understanding how forensic tools interact with different forms of evidence in cloud environments. In addition to these dimensions, studies were analysed in terms of the technical challenges they addressed, such as volatility, trust, scalability, and data complexity, as well as the types of solutions proposed, including experimental methods, conceptual models, and prototype implementations.

3.7 Reliability and Validity

To enhance the reliability of the classification process, two researchers independently performed the initial coding of the selected studies. Differences in classification were discussed and resolved through consensus, ensuring consistency in the application of the coding scheme. This approach reduces subjectivity and strengthens the validity of the results. Nevertheless, some limitations remain inherent to the methodology. The classification of studies into discrete categories may involve interpretation, particularly when studies address multiple service models or forensic phases. However, the use of a predefined framework and collaborative validation helps mitigate these concerns and supports the robustness of the mapping.

4. RESULTS AND DISCUSSION

This section presents the synthesis and critical interpretation of data extracted from the 12 primary studies. The analysis integrates the identification of studies, their classification across research dimensions, and the evaluation of technical challenges and solution approaches. Tables 1–3 and Figure 1 are used to support the interpretation of patterns and trends in the literature.

4.1 Overview of Included Studies

Following the selection process, 12 primary studies, labelled P1 to P12, were included. These studies span the period from 2020 to 2025 and collectively represent key developments in cloud forensic tools and storage-related investigation techniques. The selected works address topics including IaaS-based evidence acquisition, Zero Trust forensic architectures, container and cloud-native environments, and automated analysis of large-scale log and metadata collections. The temporal distribution reveals a transition from conceptual and challenge-driven research toward more solution-oriented and implementation-focused approaches, particularly in areas such as automated log analysis and forensic readiness.

The included studies are summarised in Table 1.

Table 1: List of Included Primary Studies (P1–P12)

ID	Title / Topic Summary	Year	Ref
P1	Forensics in Private Cloud (IaaS)	2020	[10]
P2	Cloud and Edge Computing Challenges	2021	[11]
P3	The Case for Zero Trust Digital Forensics	2022	[12]
P4	Digital Forensics for Ransomware	2023	[13]
P5	Forensic Analysis of Docker Containers	2023	[14]
P6	Forensics in Containers as a Service	2024	[15]
P7	Zero Trust Model for Evidence	2024	[4]
P8	Extracting and Analyzing Metadata	2024	[16]
P9	Review of Cloud Forensics	2025	[6]
P10	Automated Cloud Forensics for Large Log Collections	2025	[17]
P11	Intelligent Browser History Forensics	2025	[18]
P12	Two-tier Forensic Readiness for Zero Trust	2025	[19]

4.2 Mapping Across Service Models, Forensic Phases, and Artifacts

The classification of studies according to service model, forensic phase, and storage artifact is presented in Table 2. The mapping reveals a concentration of research in SaaS and generic environments, where investigators depend primarily on logs and metadata due to limited access to infrastructure. SaaS-focused studies (P4 [13], P8 [16], P10 [17], P11 [18]) emphasise analysis of application-level artifacts, while IaaS work (P1 [10]) retains elements of traditional forensic approaches. PaaS studies (P5 [14], P6 [15]) highlight container-based environments and the challenges of acquiring ephemeral data. Generic studies focus on broader issues such as trust, readiness, and system complexity. The mapping also shows that the analysis phase dominates the forensic lifecycle, with comparatively limited emphasis on acquisition and preservation.

Table 2: Mapping of Primary Studies to Research Questions

ID	Service Model	Forensic Phase	Storage Artifact
P1	IaaS	Analysis	Log Analysis
P2	Generic	Challenges	Cloud Logs
P3	Generic	Model	Zero Trust Arch
P4	SaaS	Analysis	Encrypted Files

P5	PaaS	Analysis	Docker Logs
P6	PaaS	Acquisition	Container Vol.
P7	Generic	Preservation	Evidence Hash
P8	SaaS	Analysis	Cloud Metadata
P9	Generic	Review	Legal/Tech
P10	SaaS	Analysis	Log Collections
P11	SaaS	Analysis	Web Activity
P12	Generic	Readiness	IoT/Edge Data

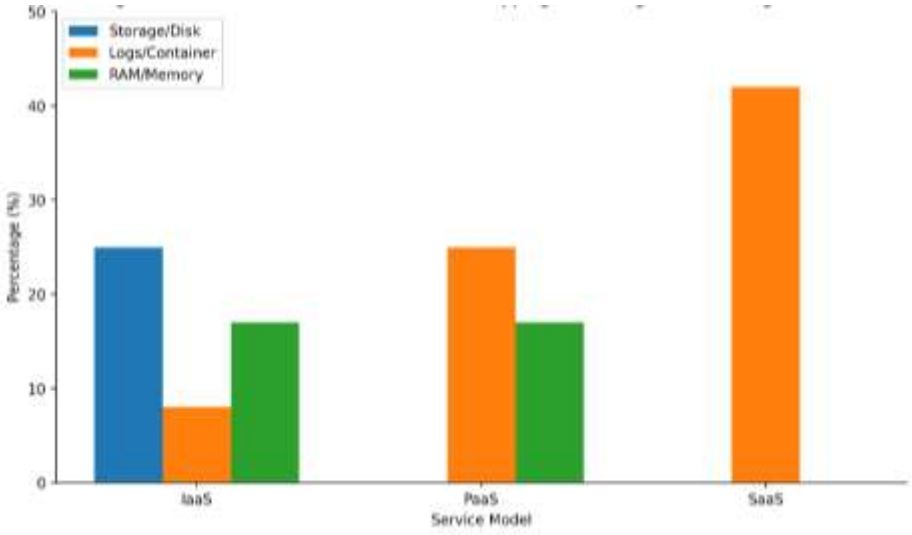
4.3 Storage Artifact Distribution and Interpretation

The distribution of storage artifacts across service models is illustrated in Figure 1. The figure captures the relative proportion of studies targeting disk-based, log-based, and memory-related artifacts within IaaS, PaaS, and SaaS environments. A clear dominance of log-based artifacts is observed, particularly in SaaS environments, where logs account for the largest proportion of evidence sources. This reflects the practical constraint that investigators in SaaS environments rely almost exclusively on application-level logs and metadata. In contrast, disk and snapshot artifacts are primarily associated with IaaS, where limited access to virtual storage is still available.

The figure also highlights the emergence of container and ephemeral artifacts within PaaS environments. Although currently less represented, these artifacts are critical in modern cloud-native systems, where evidence may exist only for short durations. Their comparatively lower proportion in Figure 1 indicates that current forensic tools are not yet fully aligned with the requirements of dynamic, container-based infrastructures.

Taken together, Figure 1 provides quantitative support for the transition from static, disk-centric forensic models to dynamic, log-centric and metadata-driven approaches, while also exposing the relative underdevelopment of techniques for handling volatile storage.

Figure 1: Illustrative distribution of studies mapping tool categories to storage artifacts across service models



This distribution quantitatively reinforces the dominance of log-centric investigation approaches and highlights the relative immaturity of techniques for handling ephemeral storage in cloud-native environments.

4.4 Analysis of Technical Challenges and Solution Approaches

The mapping of studies to technical challenges and proposed solutions is presented in Table 3. The results show three dominant categories of challenges: volatility, data scale, and trust. Volatility is addressed primarily in container-based studies (P5 [14], P6 [15]), where the short lifecycle of workloads requires rapid and automated acquisition mechanisms. Data scale is addressed through automated and data-driven analysis techniques (P1 [10], P10 [17], P11 [18]), enabling efficient processing of large log datasets. Trust and evidence integrity are addressed through Zero Trust-based approaches (P3 [12], P7 [4], P12 [19]), which introduce mechanisms for ensuring the reliability of evidence. Despite these advances, most solutions remain at the conceptual or prototype stage, with limited validation in operational environments.

Table 3: Analysis of Challenges and Proposed Solutions (SQ4)

ID	Challenge	Proposed Solution	Method
P1	Log Volume	Data-driven log reduction and triage	Experiment
P2	Complexity	Cloud and edge forensic framework	Survey
P3	Trust	Zero Trust forensic architecture	Conceptual
P4	Encryption	Identification of ransomware artifacts	Case Study
P5	Volatility	Live analysis of Docker containers	Experiment
P6	Ephemeral Data	Automated acquisition in container environments	Tool Impl.

P7	Integrity	Blockchain-based chain of custody	Model
P8	Data Hiding	Metadata extraction techniques	Experiment
P9	Legal Gaps	Review of forensic challenges	Review
P10	Analysis Speed	Automated log investigation	Prototype
P11	User Behavior	Automated browser activity analysis	Algorithm
P12	Readiness	Forensic readiness architecture	Architecture

4.5 Integrated Discussion

The combined interpretation of Tables III–V and Figure 1 shows that cloud forensic research is shaped by three interacting constraints: abstraction, scale, and volatility. Increasing abstraction limits access to infrastructure, scale necessitates automation, and volatility requires rapid acquisition mechanisms. Figure 1 reinforces this interpretation by demonstrating the dominance of log-based evidence and the limited representation of ephemeral artifacts. This highlights a gap between current forensic tools and the operational realities of modern cloud-native systems.

5. Conclusion

This study presented a systematic mapping of cloud forensic tools and storage-related investigation techniques published between 2020 and 2025. By analysing 12 primary studies, the work provides a structured and technically grounded overview of how forensic approaches are evolving across cloud service models, forensic process phases, and storage artifacts. The results demonstrate a clear transition from traditional infrastructure-centric investigations toward approaches that rely on provider-controlled interfaces and application-level data.

A central finding of this study is the dominance of log-based and metadata-driven analysis, particularly in Software-as-a-Service environments, where access to underlying infrastructure is inherently limited. While disk and snapshot analysis remain relevant in Infrastructure-as-a-Service contexts, they no longer represent the primary source of evidence in cloud investigations. At the same time, the study highlights the increasing importance of container and ephemeral storage artifacts, which introduce new complexities due to their short lifecycle and dynamic nature. The analysis further identifies three major cross-cutting challenges that shape current research: evidence volatility, data scale, and trust in cloud environments. Although existing studies propose solutions such as automated log analysis, live container forensics, and Zero Trust-based integrity mechanisms, most approaches remain at the conceptual or prototype stage. In particular, there is limited support for reliable acquisition of ephemeral data and for ensuring transparency and explainability in automated forensic processes, both of which are essential for legal admissibility.

This study contributes to the field in three main ways. First, it provides a structured classification of cloud forensic research by explicitly linking tools to service models, forensic phases, and storage artifacts. Second, it offers a systematic analysis of key technical challenges and how current approaches attempt to address them. Third, it identifies critical gaps in existing research, particularly in relation to container forensics, forensic readiness, and transparent automated analysis.

From a practical perspective, the findings suggest that future cloud forensic tools must evolve toward integrated, cloud-native frameworks that support real-time evidence capture, scalable data analysis, and verifiable integrity mechanisms. In addition, these tools must balance automation with transparency to ensure that forensic findings remain interpretable and defensible in legal contexts. However, the results of this study are based on a limited set of 12 primary studies and should therefore be interpreted as indicative trends rather than exhaustive coverage of all available tools and

approaches. Future research should focus on developing forensics-as-a-service frameworks for automated evidence preservation, cross-cloud evidence correlation mechanisms for multi-provider investigations, and explainable forensic analysis techniques that enhance both operational effectiveness and legal reliability.

References

[1] National Institute of Standards and Technology, *"NIST cloud computing forensic science challenges,"* NIST, Tech. Rep. IR 8006, 2020.

[2] K. Ruan and J. Carthy, *"Cloud forensics definitions and critical criteria,"* Digital Investigation, 2011.

[3] Docker Inc., *Docker Engine Documentation*, 2025. [Online]. Available: https://www.docker.com

[4] S. Tyagi et al., *"Zero trust model for security of evidence in cloud forensic,"* IEEE Transactions on Cloud Computing, 2024.

[5] Y. Yao et al., *"Systematic review of LLM applications in cybersecurity,"* Journal of Cybersecurity, 2025.

[6] S. Almulla et al., *"A state-of-the-art review of cloud forensics,"* Journal of Digital Forensics, Security and Law, 2025.

[7] K. Petersen et al., *"Systematic mapping studies in software engineering,"* in Proc. EASE, 2008.

[8] S. Almulla et al., *"A state-of-the-art review of cloud forensics,"* Journal of Digital Forensics, Security and Law, 2025.

[9] S. Tyagi et al., *"Zero trust model for security of evidence in cloud forensic,"* IEEE Transactions on Cloud Computing, 2024.

[10] S. Gupta et al., *"Forensics in private cloud leveraging techniques in machine learning,"* International Journal of Advanced Trends in Computer Science and Engineering, 2020.

[11] V. R. Kebande et al., *"Cloud and edge computing-based computer forensics: Challenges and open problems,"* Electronics, 2021.

[12] M. Scanlon et al., *"The case for zero trust digital forensics,"* Forensic Science International: Digital Investigation, 2022.

[13] B. A. Al-rimy et al., *"Digital forensics for ransomware-based software,"* International Journal of Open Source Software and Processes, 2023.

[14] J. Franco et al., *"Forensic analysis of cryptojacking in host-based docker containers,"* in Proc. IEEE International Conference on Communications, 2023.

[15] L. Elie et al., *"Optimising digital forensics investigations in containers as a service environments,"* National College of Ireland Repository, 2024.

[16] S. Gulyamov et al., *"Methods of extracting and analyzing metadata for evidentiary purposes,"* Uzbek Journal of Law and Digital Policy, 2024.

[17] A. Researcher et al., *"LLM-powered automated cloud forensics: From log analysis to investigation,"* in Proc. IEEE International Conference on Cloud Engineering, 2025.

[18] B. Author et al., *"An intelligent browser history forensics method for automated analysis of web activity logs,"* Preprints, 2025.

[19] C. Researcher et al., *"Two-tier forensic readiness architecture for zero trust-enabled Industry 4.0 applications,"* Journal of Information Security and Applications, 2025.