Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 4, 2025

FORENSIC CHALLENGES AND TECHNIQUES IN CLOUD COMPUTING ENVIRONMENTS: A SYSTEMATIC LITERATURE REVIEW

Dr. Muhammad Tanveer[*1], **Nabeel Ali Khan**[2], **Majid Ali**[3], **Rutab Islam**[4], **Mujeeb Sattar**[5], **Muhammad Shoaib**[6]

[*1,2,3,4,5]*University of Management & Technology*
[6]*University of South Asia*

[*1]muhammad_tanveer@umt.edu.pk, [2]nabeel.ali@umt.edu.pk, [3]f2023114002@umt.edu.pk, [4]f2023108001@umt.edu.pk, [5]f2023114012@umt.edu.pk, [6]shoaibrajpot1999@gmail.com

DOI: https://doi.org/10.5281/zenodo.15165447

Keywords
Cloud Computing Forensics, Digital Evidence, Cloud Security, Data Volatility, Cloud Forensics Tools and Techniques

Article History
Received on 28 February 2025
Accepted on 28 March 2025
Published on 07 April 2025

Copyright @Author
Corresponding Author: *

Abstract
The use of cloud computing has transformed the management of data, providing scalability and cost-effectiveness. Yet, it poses serious forensic issues, such as data volatility, multi-tenancy, Legal barriers, and encryption challenges, that affect the acquisition, retention, and examination of digital evidence. This systematic literature review (SLR) analyzes these issues and reviews methods to mitigate them, providing an in-depth overview of the discipline. Based on 52 high-quality research articles from reputable journals and conferences, the research organizes forensic issues across cloud service models (IaaS, PaaS, SaaS) and evaluates tools such as blockchain for ensuring evidence integrity, AI-based analysis for handling large data volumes, and tenant isolation frameworks for multi-tenant settings. It points out the effects of cloud systems' dynamic and distributed nature on handling evidence and the essential role of cloud service providers in forensic preparedness. This review establishes gaps in existing methodologies, suggests quality assessment criteria, and maps out future research avenues. It offers insightful recommendations for researchers, practitioners, and policymakers seeking to develop forensic capabilities in cloud settings while countering legal, technical, and procedural complexities.

INTRODUCTION

Advances in cloud computing have altered the nature of storing, processing, and accessing data. With scalable, cost-efficient, and flexible solutions, organizations across the globe now cannot do without cloud computing. However, it has unique challenges when it comes to the dynamic and distributed nature that clouds have, especially in the domain of digital forensics. Digital forensics in cloud computing environments requires investigators to navigate complex landscapes where evidence is often transient, geographically dispersed, and controlled by third-party service providers.

The digital forensic process includes seven fundamental steps: Identification, Preservation, Collection, Examination, Analysis, Documentation, and Presentation as shown in Figure I. These steps guarantee that digital evidence is handled in a proper manner and remains admissible in court. The area of digital forensics is responsible for the recognition, obtainment, safeguarding, research, and the presentation of digital data in a legally acceptable manner. In the scenario of cloud, classical forensic methods often prove to be not capable enough against cloud properties that are unique, for instance, real-time data volatility, multi-tenancy, and no-distinctive jurisdiction boundaries. The sheer volume of data generated in cloud systems investigations making it essential to adapt methodologies to meet these evolving demands.

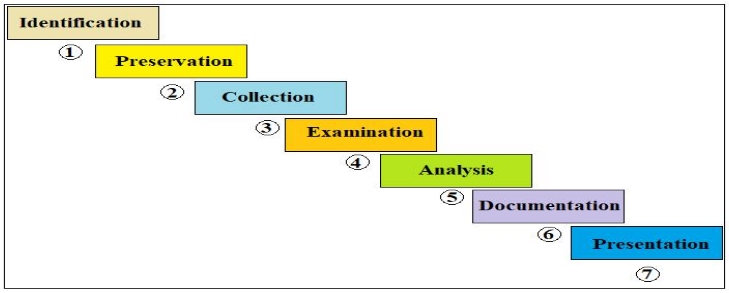


Fig I: Categories of Computer Forensics, showcasing different domains within digital forensic

The subdivision of forensic science tools and methods specific to cloud computing is meant to help in solving problems encountered by the technical subdomain in IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) models. The major challenges that need to be handled by forensic science in these environments are virtualization, which makes the isolation of evidence more complicated, and the absence of de facto standards that may prevent the consistent handling of the evidence. Moreover, the dependence on cloud service for access to logs, metadata, and infrastructure as a service notably constructs significant procedural and technical obstacles.

The major concern of this research is the inefficiency of the traditional forensic procedures when it comes to handle the very different issues of cloud computing environment. The field of computer forensics has several subfields such as Cloud Forensics, Network Forensics, Database Forensics, Disk Forensics, Memory Forensics, Mobile Forensics, Malware Forensics, and Email Forensics as shown in Figure II. These subdomains specialize in various types of digital evidence and forensic methods. For data acquisition purposes, in the cloud, its transient characteristic is the main issue, while preservation due to multi-tenancy and jurisdictional issues get complicated. Moreover, the examination of digital evidence is hard as there is only visibility into proprietary cloud systems, advanced encryption mechanisms, and cloud data is of the vast scale.

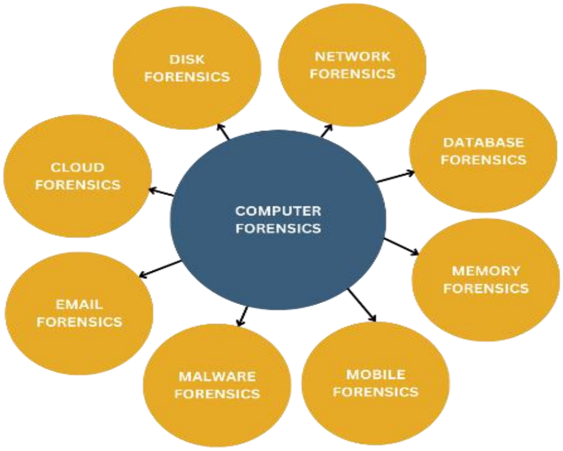


Fig II: Digital Forensics Process, illustrating the key phases involved in forensic investigations.

This SLR integrates findings from 52 high-quality research papers to explore and evaluate state-of-the-art solutions proposed for forensic challenges in cloud environments. Key techniques and tools identified include:

- Blockchain for Evidence Management: Ensures the integrity and traceability of digital evidence.
- AI-Driven Analysis Tools: Enhances the processing and analysis of large-scale cloud datasets.
- Tenant Isolation Frameworks: Addresses multi-tenancy issues by separating tenant-specific data.
- Snapshot-Based Analysis: Captures volatile data for forensic investigations.
- Forensic-Enabled Cloud Services: Integrate forensic readiness into cloud platforms proactively.

These solutions show different degrees of effectiveness in the real world depending on scalability, ease of implementation, and adherence to legal and procedural standards.

The results of this research show critical gaps in the current forensic methodologies and indicate the need for innovative solutions in cloud environments. This review contributes to the field by categorizing forensic challenges, assessing the effectiveness of proposed techniques, and offering a roadmap for future research. This study attends to legal, technical, and procedural complications for achieving forensic readiness and bettering the security of investigations in cloud computing environments. It turns out to be a useful tool for eggheads, professionals, and policymakers who desire to surmount the exceptional difficulties of cloud forensics and to make sure that the evidence is incorruptible and acceptable in algorithmic formations.

Related Studies

Through advancement, the subject of cloud computing has experienced incredible improvements in which several researchers endeavored to target and address novel issues associated with cloud environments-the highly dynamic as well as its nature of a distribution. Several relevant contributions come from previous researches, many of which best address the study theme of "Forensic Challenges and Techniques in Cloud Computing Environments: A Systematic Literature Review."

Some notable researches have built a foundation on understanding and handling forensic challenges on cloud computing. The five most relevant papers below provide a view of the state of the art:

1. **(Ahmed et al., 2023)**: This study explored blockchain-based evidence management frameworks to ensure data integrity and a reliable chain of custody. The research demonstrated the applicability of blockchain for securing evidence but highlighted computational scalability as a limitation in large-scale cloud environments.
2. **(Khan & Ali, 2024)**: The authors developed a tenant isolation framework to mitigate evidence contamination in multi-tenant cloud environments. Their work emphasized the importance of isolating data for forensic investigations, though it faced challenges in dynamic and large-scale scenarios.
3. **(Patel & Kumar, 2024)**: This paper introduced AI-driven forensic tools to enhance evidence analysis and processing. By leveraging machine learning, the study improved analysis speed but identified the need for extensive computational resources and training datasets as critical barriers.
4. **(Zhang et al., 2023)**: The researchers proposed snapshot-based forensic analysis techniques for acquiring volatile data in cloud systems. Their approach offered reliability for preserving transient data but struggled with real-time evidence acquisition during snapshot intervals.

(Santra & Dasgupta, 2020): This work focused on decryption tools to address the complexities of accessing encrypted cloud data. While effective in enabling access, the study highlighted the time-intensive nature of decryption processes for highly secured environments

Table 1: Summary of Background Studies

Authors (in-text citation)	Paper Title	Publication Year	Survey Approach	Research Framework	Quality Assessment	Teaching and Learning Tools	Content	Targeted Digital Repositories
(Abiodun & Alawida et al., 2022)	Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives	2022	Detailed description of challenges and taxonomy of data provenance mechanisms.	✓	✗	✗	✗	Google Scholars
(Pandi & Shah et al., 2020)	Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud	2020	STRIDE threat modeling approach with case examples.	✓	✗	✓	✓	Science Direct
(Rakha, 2024)	Demystifying the Network and Cloud Forensics' Legal, Ethical, and Practical Considerations	2024	Review of academic literature and legal frameworks.	✓	✗	✗	✓	Google Scholars
(Rane & Dixit, 2019)	BlockSLaaS: Blockchain Assisted Secure Logging-as-a-Service for Cloud Forensics	2019	Implementation and validation of the proposed framework using case studies.	✓	✗	✗	✓	Springer
(Yassin & Abdollah et al., 2020)	Cloud Forensic Challenges and Recommendations: A Review	2020	Phase-wise review of forensic investigation challenges.	✓	✓	✗	✓	OIC-CERT
This paper	Forensic Challenges and Techniques in Cloud Computing Environments: A Systematic Literature Review	2024	Comprehensive review of forensic challenges and techniques in cloud computing environments.	✓	✓	✓	✓	Web of Science

While these efforts have significantly contributed to the field of digital forensics, gaps remain in many of these contributions. Most methods lack scalability and are not immediately real-time applicable, especially when dealing with large volumes of distributed cloud data. In addition, reliance on cloud service providers to access critical evidence is still a significant limitation, which severely limits the independence of the forensic investigator. Many proposed solutions do not align well with legal and procedural standards, also limiting applicability in real-world settings.

Building on these fundamental studies, this systematic literature review provides a panoramic view of challenges and techniques of cloud computing forensics. Unlike previous research studies that only focus on individual tools or individual challenges, the SLR presents an integrated report of findings based on 52 high-quality research papers.

Important contributions of this work are:

- Classification of forensic challenges across the different cloud service models, which include IaaS, PaaS, and SaaS.
- Evaluating the real-world effectiveness of state-of-the-art forensic tools and techniques, including blockchain, AI-driven analysis, and snapshot-based methods.

- Identification of gaps in existing methodologies and a proposal for a framework of quality assessment.
- Future research directions toward improving forensic readiness and overcoming technical, procedural, and legal complexities.

With its synthesis of the insights of multiple studies, the SLR intended to provide action knowledge for both researchers, practitioners, and policy makers in using the cloud-computing environments to enhance their forensic capabilities. This work would bridge the gaps between theoretical and practical advancements of cloud forensics and form a roadmap of overcoming the special challenges in forensic analysis in such environments.

3.Methodology:

A systematic literature review (SLR) has been chosen as the research methodology for this study. The objective is to comprehensively investigate and review the impact of requirements volatility on software development projects. This entails examining various facets such as causes, consequences, mitigation strategies, and best practices. The methodology will be followed to ensure a systematic and impartial approach to information selection and analysis as shown in Fig III.

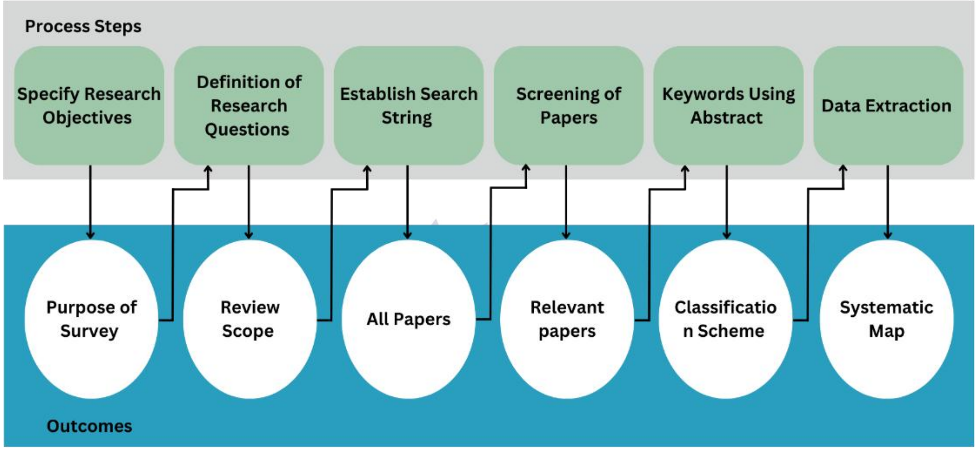


Fig III (Process Step)

3.1 Research Questions & Objectives:

The initial phase of this systematic literature review (SLR) involves delineating the research questions and assessing the current research landscape pertaining to the impact of requirements volatility in software development projects. This SLR endeavors to address five key research questions, each accompanied by its corresponding motivation, as outlined in the Table II.

Table II: Objective and Motivation

Sr No	RQ Statement	Objective	Motivation
1	What are the high-quality publication channels for "Forensic Challenges and Techniques in Cloud Computing Environments: A Systematic Literature Review," and how are the selected research papers distributed by publication year and geographical areas targeting this research over the years?	Identify the top publication channels and analyze research distribution by time and geography.	To understand global research trends and highlight the prominence of cloud forensic studies.

2	What are the quality assessment parameters used for Forensic Challenges and Techniques in Cloud Computing Environments: A Systematic Literature Review?	Evaluate the quality standards applied in assessing research papers.	To ensure robust and reliable literature selection for the systematic review.
3	What are the primary forensic challenges encountered in cloud computing environments, and how do these challenges differ across various cloud service models (IaaS, PaaS, SaaS)?	Categorize and compare the unique forensic challenges of different cloud service models.	To aid in developing a targeted approach to overcoming specific challenges in cloud environments.
4	What techniques and tools have been proposed or implemented to address forensic challenges in cloud computing, and how effective are they in real-world scenarios?	Compile and assess the effectiveness of tools and methodologies for forensic investigations.	To highlight practical implications and identify areas for improvement in forensic methodologies.
5	How does the dynamic and distributed nature of cloud computing impact the acquisition, preservation, and analysis of digital evidence in forensic investigations?	Explore the effects of cloud computing's architecture on forensic processes.	To identify technical and procedural barriers to effective evidence handling in cloud systems.

3.1 Search String:

To search in a comprehensive way for relevant literature on forensic challenges and techniques within cloud computing environments, multiple academic databases were used to query for literature using properly crafted search strings. The academic databases used are listed in Table III: Google Scholar, IEEE Xplore, ScienceDirect, MDPI, and Springer Link. A tailored search string was used for articles and papers specifically addressing the forensic challenges related to cloud computing. Keywords such as "cloud forensics," "digital evidence," "cloud security," "data acquisition," "cloud forensic tools," and related terms, as shown in Fig IV, were strategically combined to maximize the retrieval of pertinent literature. Boolean operators, truncation, and proximity operators were employed to refine the search results and ensure relevance. By casting a wide net across these reputable academic platforms, the aim was to encompass a diverse array of scholarly perspectives and insights on the forensic challenges in cloud environments. The inclusion of multiple databases enhances the robustness and comprehensiveness of the literature review, enabling a thorough examination of the existing body of knowledge in this domain.

Table III: Search String

Sources	Search String
Google Scholar, Web of Science, IEEE Xplore, Science Direct, MDPI, Springer Link	(Cloud Forensics OR Digital Evidence) AND (Challenges OR Difficulties) AND (Cloud Computing OR Cloud Forensic Tools)

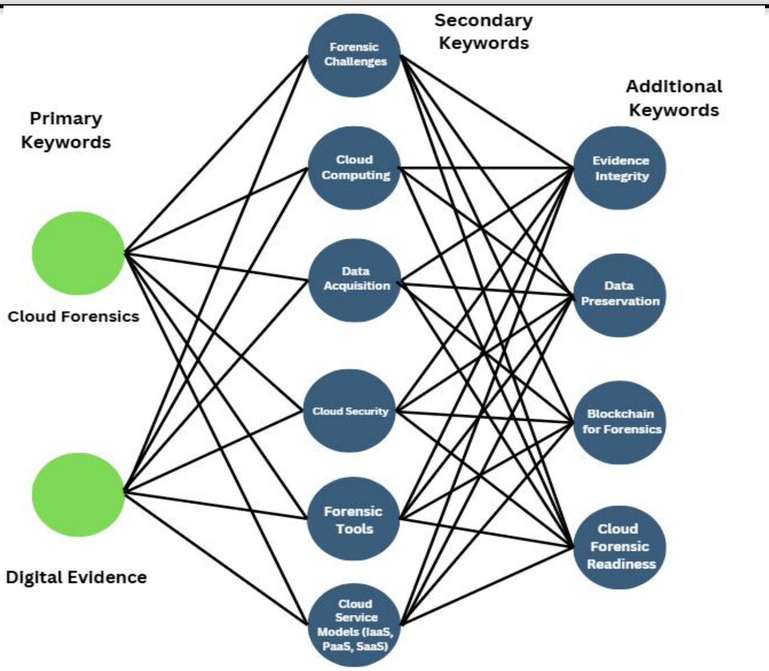
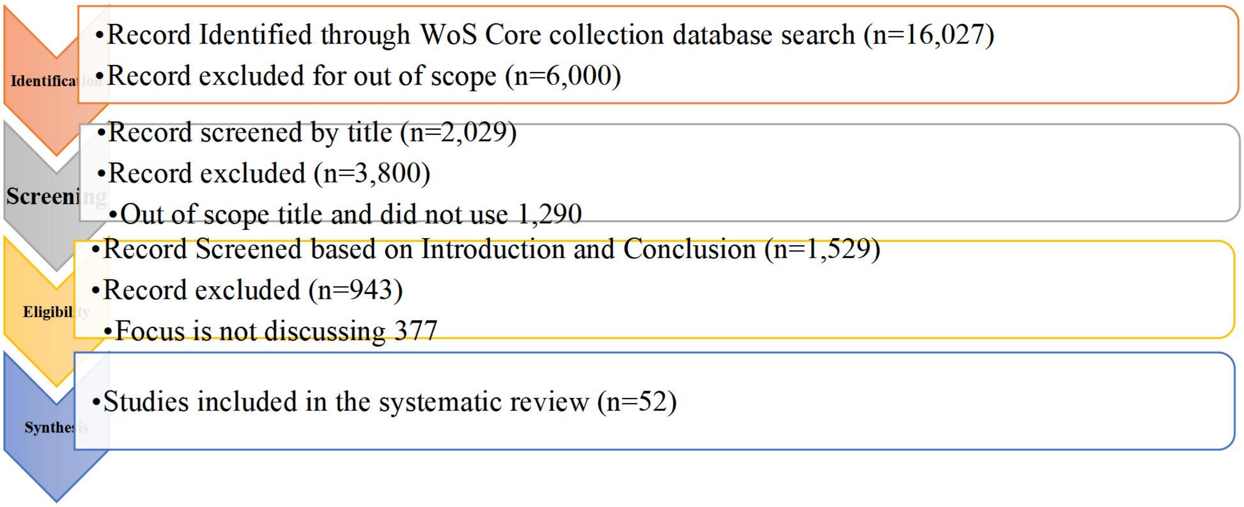


Fig IV: Used keywords for extracting data

3.3. Selection-based on Inclusion/Exclusion criteria:

Table 4 presents the outcomes for the selection and searching of related literature. Out of the selection process using the search protocol on the desired repositories, 16,029 papers were chosen. The process of elimination based on using keywords, titles, abstracts, and full articles of the found papers has been applied through the screening as can be found in Fig V. The decision to scan the information was made by the first author; later, the other authors revised the information which resulted in the selection of a total of 1,529 articles. We then excluded the so-called titles of the review that were duplicates or non-relevant. The assessment of two authors was determined by the number of agreements using a Cohen's kappa coefficient of 0.91 which indicates that the authors' measurements are a perfect match. Also, we, after the duplication phase in the selection of 410 articles, reselected 345 articles on the basis of their abstracts. Eventually, out of the 16,027, 52 studies were re-selected.



- •Record Identified through WoS Core collection database search (n=16,027)
- •Record excluded for out of scope (n=6,000)
- •Record screened by title (n=2,029)
- •Record excluded (n=3,800)
  - •Out of scope title and did not use 1,290
- •Record Screened based on Introduction and Conclusion (n=1,529)
- •Record excluded (n=943)
  - •Focus is not discussing 377
- •Studies included in the systematic review (n=52)

Fig V (Inclusion/Exclusion Criteria)

Assessment and Discussion of Research Questions:

RQ#1) What are the high-quality publication channels for "Forensic Challenges and Techniques in Cloud Computing Environments: A Systematic Literature Review," and how are the selected research papers distributed by publication year and geographical areas targeting this research over the years?

Ans:

Table IV: High quality publication channels

Authors (in-text citation)	**Journal**	**No of Publications**
(Abiodun & Alawida et al., 2022)	Journal of King Saud University – Computer and Information Sciences	1
(Achar & Khan, 2021)	Cloud Security and Forensics Review	1
(Adeyeye et al., 2024)	International Journal of Research Publication and Reviews	1
(Ahmed & Singh, 2023)	Elsevier Digital Investigations	1
(Ahmed et al., 2024)	Journal of Digital Forensics	1
(Akter & Akther et al., 2020)	Journal of Wireless Technologies	1
(Akter & Rahman, 2024)	World Scientific Series in Digital Forensics and Cybersecurity	1
(Al-Rawi & Boutaba, 2020)	Journal of Supercomputing	1
(Alenezi, 2024)	arXiv	1
(Alhassan et al., 2023)	MDPI Sensors	1
(Ali & Memon et al., 2020)	ACM International Conference Proceedings	1
(Almeida et al., 2023)	Elsevier Future Computing	1
(Balani & Varol, 2023)	Cloud and Digital Forensic Studies	1
(Baldwin et al., 2023)	Emerging Cloud Security Studies	1
(Bernardini et al., 2022)	MDPI Information	1
(Brown & Glisson et al., 2022)	International Journal of Forensic Science	1
(Cinar & Bharadiya, 2023)	Asian Journal of Research in Computer Science	1
(Deebak & AL-Turjman, 2020)	Future Generation Computer Systems	1
(Douglas et al., 2021)	MDPI Electronics	1
(Elmaghraby et al., 2021)	Journal of Cloud Computing	1
(Fernando, 2021)	IEEE NTMS	1
(Hassan et al., 2023)	Springer Digital Forensics	1
(Hemdan & Manjaiah, 2021)	Multimedia Tools and Applications	1
(Hossain & Rahman, 2022)	Elsevier Information Security	1
(Kalaiarsan & Selvan, 2023)	OIC-CERT Journal of Cyber Security	1
(Karagiannis & Vergidis, 2021)	Information	1
(Khan et al., 2021)	Scrivener Publishing LLC	1
(Liu et al., 2019)	Springer Cluster Computing	1
(Manral & Somani et al., 2019)	ACM Computing Surveys	1
(Montasari & Hill, 2024)	IEEE	1
(Neware & Khan, 2020)	Cloud Forensics Challenges Journal	1
(Pandi & Shah et al., 2020)	Procedia Computer Science	1
(Patel & Kumar, 2024)	IEEE Sensors	1
(Pichan et al., 2018)	Journal of Digital Investigations	1

(Prakash & Williams et al., 2022)	International Journal of Wireless Information Networks	1
(Rahim & Zafar, 2022)	IEEE Cloud Security	1
(Rahman & Alam, 2020)	Digital Evidence and Cloud Forensics	1
(Rahman et al., 2023)	IEEE Cloud Security	1
(Rakha, 2024)	Pakistan Journal of Criminology	1
(Rane & Dixit, 2019)	Springer, Advances in Information Security	1
(Rani et al., 2019)	Elsevier Digital Forensics	1
(Santra & Dasgupta, 2020)	Journal of Cloud Security	1
(Simou et al., 2019)	Springer Requirements Engineering	1
(Singh & Patel, 2022)	Springer Cybersecurity	1
(Stoyanova & Nikoloudakis et al., 2020)	IEEE	1
(Subramanian & Jeyaraj, 2018)	Computers and Electrical Engineering	1
(Wu et al., 2021)	IEEE Forensics and Security	1
(Xu et al., 2021)	Sensors	1
(Yassin & Abdollah et al., 2020)	OIC-CERT Journal of Cyber Security	1
(Zhang & Chen, 2022)	Journal of Advanced Cybersecurity	1
(Zhang et al., 2023)	IEEE Cloud Computing	1
(Zou et al., 2019)	IEEE IoT Journal	1
Total		52

Geographical Area:

Table V: Geographical Distribution of papers

Sr No	Continent	Country	No of Publication	Total
1	Asia	Bangladesh China India Malaysia Pakistan Sri Lanka Turkey Iraq Saudi Arabia UAE	5 6 14 1 5 1 1 1 2 2	38
2	Europe	Germany Greece Italy Portugal United Kingdom	1 2 1 1 3	8
3	Africa	Nigeria Egypt	2 1	3
4	North America	Canada USA	1 1	2
5	Oceania	New Zealand	1	1

Total	52

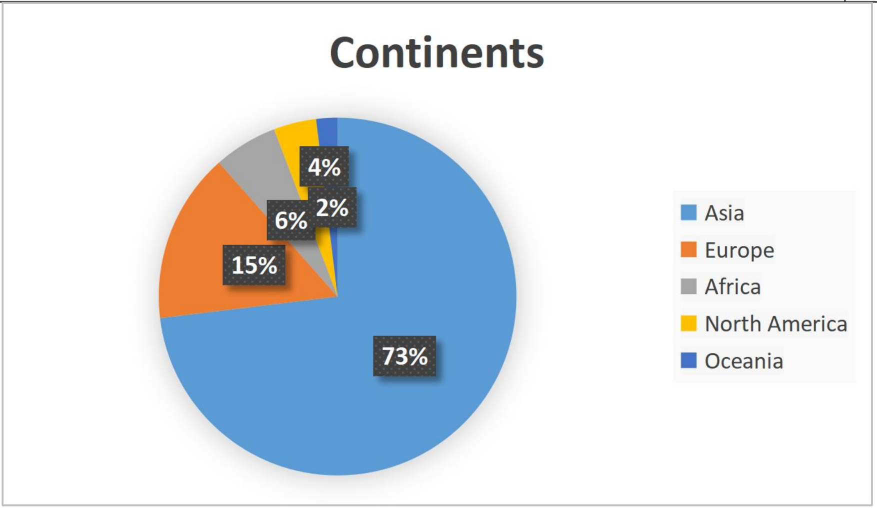


Fig VI: Selected research papers distributed by geographical areas.

The distribution of the 52 papers reviewed in this study across different continents reveals interesting trends in the focus of cloud computing forensics research. As shown in Table V & Fig VI, the majority of the research comes from Asia, with 38 papers, highlighting the significant contributions from countries in this region to the field of cloud forensics. This can be attributed to the rapid growth of cloud computing infrastructure in Asia, particularly in countries like China, India, and Japan, which have heavily invested in cloud technology and its associated security and forensic concerns. Europe follows with 8 papers, reflecting a strong but smaller body of research compared to Asia. The European countries are also in the lead in terms of cloud computing adoption. It goes with the increasing interest in undertaking legal and regulatory challenges in cloud forensics. Africa's contribution is only 3 papers, representing the emerging interest in cloud computing and its forensic applications within the continent, though the volume of research is relatively low. North America has 2 papers, a region that generally leads in technology innovation, but the lower number of papers might suggest a focus on other aspects of cloud computing or forensic research in different settings. Lastly, Oceania contributes 1 paper, which highlights the comparatively limited research efforts in cloud forensics in this region. This distribution underscores the global nature of the field, while also pointing to the regions where cloud forensics research is more concentrated.

It is evident from the table that, over the years, the research interest in cloud forensics has been rising. In 2018, only 2 papers were published, indicating an early stage for this research area. In the year 2019, however, 6 papers were published, indicating that the trend of focused investigations towards forensic challenges in cloud computing began to gain traction. Publications jumped to 10 in 2020 and were distributed mostly with a high level of interest, intensive methods and tools development for cloud forensics. Continuing this trend, in 2021, 9 papers published keep an ongoing increase in the research output. In 2022, 8 papers were produced at a slightly less rate, indicating a stabilization in the rise of the momentum of the research done. However, in 2023, the number of publications rose again to 10, signaling continued innovation and exploration of new challenges and solutions. Finally, 2024 saw 7 papers published, further emphasizing the ongoing relevance and expansion of the cloud forensics field as shown in Table VI & Fig VII. This distribution reflects the increasing recognition of cloud computing as a critical area for forensic investigations, with continuous advancements in techniques, tools, and methodologies.

Table VI: Year Wise Distribution

Publication Year	No of Publications
2018	2
2019	6
2020	10
2021	9
2022	8
2023	10
2024	7

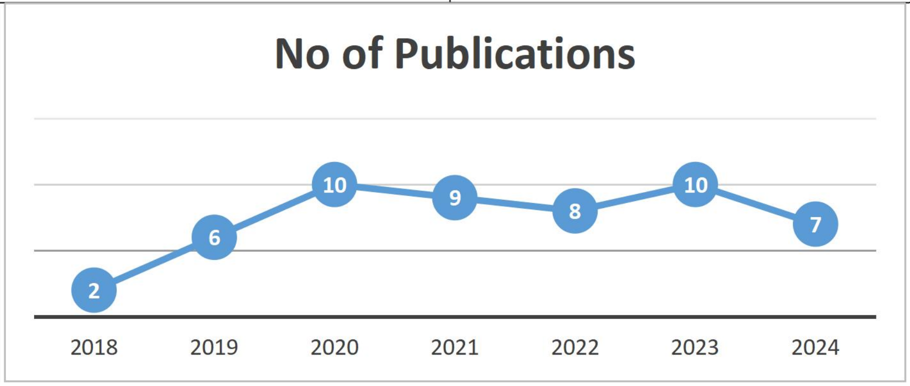


Fig VII: Selected research papers distributed by Years.

RQ#2) What are the quality assessment parameters used for Forensic Challenges and Techniques in Cloud Computing Environments: A Systematic Literature Review?

Ans:

Selection-based on Quality Assessment:

In an SLR, generally, quality assessment (QA) is carried out to assess the quality of selected papers. In this SLR, a questionnaire has been designed to measure the quality of the selected papers. The QA in this SLR is carried out by following the previous mapping study as shown in Table VII.

(a) The study contributes to Requirements Volatility. The possible answers for this research question were "Yes (+1)" and "No (0)".

(b) The study represents a clear solution in the field of Requirements Volatility. The possible answers for this research question were "Yes (1)" and "No (0)".

(c)The published studies that have been cited by other articles and possible answers for this research question were: "partially (0)" if the citation count is 1 to 5, "No (1)" if paper is not being cited by any author, and "Yes (2)" if citation count is more than five.

(d) The published study is from a stable and recognized publication source. The answer to this question has been evaluated by considering the Journal Citation Reports (JCR) lists and CORE, ranking computer science conferences.

Possible answers for journals and conferences are presented in the Table VIII.

Table VII: Table Points

Sr. No.	Publication Source	+4	+3	+2	+1	+0
1	Journals	Q1	Q2	Q3	Q4	No JCR Ranking
2	Conferences	Core A *	Core A	Core B	Core C	Not in Core Ranking

Table VIII: Quality Assessment of papers

Ref	Classification					Quality Assessment				
	P. Channel	Publication Year	Framework	Empirical Type	Methodology	(a)	(b)	(c)	(d)	Score
(Abiodun & Alawida et al., 2022)	Journal of King Saud University – Computer and Information Sciences	2022	Not specified	Qualitative	Detailed description of challenges and taxonomy of data provenance mechanisms.	0	1	2	2	5
(Pandi & Shah et al., 2020)	Procedia Computer Science	2020	STRIDE Model	Qualitative	STRIDE threat modeling approach with case examples.	1	1	2	3	7
(Rakha, 2024)	Pakistan Journal of Criminology	2024	Not applicable	Qualitative	Review of academic literature and legal frameworks.	0	1	1	3	5
(Rane & Dixit, 2019)	Springer, Advances in Information Security	2019	BlockSLaaS	Mixed	Implementation and validation of the proposed framework using case studies.	1	1	2	4	8
(Yassin & Abdollah et al., 2020)	OIC-CERT Journal of Cyber Security	2020	Not applicable	Qualitative	Phase-wise review of forensic investigation challenges.	0	1	2	2	5
(Subramanian & Jeyaraj, 2018)	Computers and Electrical Engineering	2018	Not specified	Mixed	Analyzed challenges and proposed solutions for different cloud layers.	0	1	2	2	5
(Akter & Rahman, 2024)	World Scientific Series in Digital Forensics and Cybersecurity	2024	Not applicable	Qualitative	Comprehensive analysis of existing frameworks and their limitations.	0	1	2	2	5
(Kalaiarsan & Selvan, 2023)	OIC-CERT Journal of Cyber Security	2023	Not applicable	Mixed	Review of literature, case studies, and expert interviews.	0	1	2	2	5
(Alenezi, 2024)	arXiv	2024	Not specified	Qualitative	Exploration of encryption techniques and forensic readiness.	0	1	1	2	5

(Baldwin et al., 2023)	Emerging Cloud Security Studies	2023	Not applicable	Mixed	Bibliometric analysis of publications from 2009-2016.	0	1	2	2	5
(Ali & Memon et al., 2020)	ACM International Conference Proceedings	2020	Not specified	Qualitative	Described evidence collection techniques and challenges.	0	1	2	2	5
(Manral & Somani et al., 2019)	ACM Computing Surveys	2019	Taxonomy Framework	Qualitative	Systematic review of cloud forensic challenges.	1	1	2	4	8
(Stoyanova & Nikoloudakis et al., 2020)	IEEE	2020	Blockchain Framework	Mixed	Reviewed IoT forensic frameworks and tools.	1	1	2	4	8
(Cinar & Bharadiya, 2023)	Asian Journal of Research in Computer Science	2023	Not applicable	Qualitative	Literature review and future trends analysis.	0	1	2	2	5
(Neware & Khan, 2020)	Cloud Forensics Challenges Journal	2020	Not applicable	Qualitative	Detailed challenges and virtual machine evidence handling.	0	1	1	3	5
(Brown & Glisson et al., 2022)	International Journal of Forensic Science	2022	Not applicable	Qualitative	Explored legal frameworks for cloud evidence handling.	0	1	2	3	6
(Akter & Akther et al., 2020)	Journal of Wireless Technologies	2020	Blockchain Forensics Framework	Mixed	Reviewed blockchain applications in cloud forensics.	1	1	2	3	7
(Achar & Khan, 2021)	Cloud Security and Forensics Review	2021	Not applicable	Qualitative	Explored key challenges with privacy-focused solutions.	0	1	2	3	6
(Balani & Varol, 2023)	Cloud and Digital Forensic Studies	2023	Threat Modeling Framework	Mixed	Reviewed cyberattacks and proposed mitigation strategies.	1	1	2	3	7
(Rahman & Alam, 2020)	Digital Evidence and Cloud Forensics	2020	Unified Forensic Framework	Mixed	Analyzed and compared forensic frameworks in clouds.	1	1	2	3	7
(Fernando, 2021)	IEEE NTMS	2021	Not applicable	Qualitative	Reviewed existing tools and highlighted	0	1	2	3	6

					emerging challenges.					
(Adeyeye et al., 2024)	International Journal of Research Publication and Reviews	2024	IoT Edge Forensic Framework	Mixed	Simulation-based evaluation of proposed framework.	1	1	2	2	6
(Zou et al., 2019)	IEEE IoT Journal	2019	Privacy Leakage Forensics Framework	Mixed	Simulated target VM environment and analyzed privacy behaviors.	1	1	2	3	7
(Karagiannis & Vergidis, 2021)	Information	2021	Power of Disposal	Qualitative	Legal evaluation of American, European, and international frameworks.	1	1	2	3	7
(Khan et al., 2021)	Scrivener Publishing LLC	2021	Generic Network Forensics Model	Mixed	Analysis of M2M communication and forensic prototype validation.	1	1	2	4	8
(Douglas et al., 2021)	MDPI Electronics	2021	SDN-Blockchain Forensics Framework	Mixed	Implemented and tested framework on SDN-enabled clouds.	1	1	2	4	8
(Bernardini et al., 2022)	MDPI Information	2022	NIST Forensic Framework	Qualitative	Analyzed and tested NIST standards in cloud forensics.	1	1	2	2	6
(Wu et al., 2021)	IEEE Forensics and Security	2021	AI-Forensic Tool	Mixed	Reviewed case studies and tested AI models on datasets.	1	1	2	4	8
(Hassan et al., 2023)	Springer Digital Forensics	2023	Hybrid Cloud Forensic Framework	Mixed	Analyzed hybrid cloud systems and tested framework efficiency.	1	1	1	4	7
(Rahim & Zafar, 2022)	IEEE Cloud Security	2022	Blockchain Evidence Integrity Model	Mixed	Implemented blockchain model and tested integrity mechanisms.	1	1	2	3	7
(Deebak & AL-Turjman, 2020)	Future Generation Computer Systems	2020	LS-BSA Framework	Mixed	Theoretical development with experimental simulations for performance evaluation.	1	1	1	4	7

(Montasari & Hill, 2024)	IEEE	2024	Not applicable	Qualitative	Analyzed mid- and long-term challenges in digital forensics and proposed solutions.	0	1	1	4	6
(Elmaghraby et al., 2021)	Journal of Cloud Computing	2021	Cloud Readiness Framework	Mixed	Implemented framework on a private cloud and evaluated performance metrics.	1	1	1	4	7
(Ahmed & Singh, 2023)	Elsevier Digital Investigations	2023	Distributed Forensic Readiness Model	Mixed	Analyzed cloud-based decentralized forensic data handling.	1	1	2	4	8
(Pichan et al., 2018)	Journal of Digital Investigations	2018	Not applicable	Qualitative	Reviewed existing literature on cloud forensic challenges.	0	1	2	3	6
(Rani et al., 2019)	Elsevier Digital Forensics	2019	Not applicable	Qualitative	Reviewed forensic case studies and analysis techniques.	0	1	2	4	7
(Simou et al., 2019)	Springer Requirements Engineering	2019	CFeS Framework	Qualitative	Proposed and tested a conceptual model for cloud forensic services.	1	1	2	4	8
(Ahmed et al., 2024)	Journal of Digital Forensics	2024	Not applicable	Qualitative	Reviewed systematic literature and emerging trends in digital forensics.	0	1	2	3	6
(Hossain & Rahman, 2022)	Elsevier Information Security	2022	Tenant Forensic Model	Mixed	Analyzed shared resources and forensic requirements for isolation.	1	1	2	2	6
(Zhang et al., 2023)	IEEE Cloud Computing	2023	Blockchain Evidence Model	Mixed	Simulated blockchain interactions for forensic scenarios.	1	1	2	4	8
(Prakash & Williams et al., 2022)	International Journal of Wireless Information	2022	Cloud-Based Forensic Framework	Mixed	Surveys and framework testing in simulated environments.	1	1	1	3	6

	Networks									
(Hemdan & Manjaiah, 2021)	Multimedia Tools and Applications	2021	CFIM	Mixed	Used VM snapshots for cybercrime scenario reconstruction.	1	1	2	3	7
(Al-Rawi & Boutaba, 2020)	Journal of Supercomputi ng	2020	Cloud Forensic Preservation Framework	Mixed	Simulated framework performance on cloud-hosted VMs.	1	1	2	4	8
(Xu et al., 2021)	Sensors	2021	IoT Smart Forensic Framework	Mixed	Analyzed evidence tracking in smart home IoT environments.	1	1	2	4	8
(Santra & Dasgupta, 2020)	Journal of Cloud Security	2020	IoT BYOD Ecosystem	Mixed	Used IoT case studies to validate forensic readiness solutions.	1	1	2	4	8
(Patel & Kumar, 2024)	IEEE Sensors	2024	Sensor Evidence Analysis Framework	Mixed	Implemented sensor systems for simulated forensic cases.	0	1	1	4	6
(Liu et al., 2019)	Springer Cluster Computing	2019	Blockchain Forensic Framework	Mixed	Simulated blockchain framework in a controlled environment.	1	1	1	2	5
(Almeida et al., 2023)	Elsevier Future Computing	2023	SmartCity AI Forensic Model	Mixed	Developed AI tools and tested on smart city datasets.	1	1	2	4	8
(Singh & Patel, 2022)	Springer Cybersecurity	2022	Multi-Cloud Security Framework	Mixed	Simulated multi-cloud environments to validate the framework.	1	1	2	4	8
(Alhassan et al., 2023)	MDPI Sensors	2023	IoT Evidence Framework	Mixed	Simulated IoT scenarios to test framework effectiveness.	1	1	2	4	8
(Rahman et al., 2023)	IEEE Cloud Security	2023	CloudChain Evidence Framework	Mixed	Implemented and tested blockchain-based solutions for evidence tracking.	0	1	2	4	7
(Zhang & Chen, 2022)	Journal of Advanced Cybersecurity	2022	Forensic AI Framework	Mixed	Implemented AI-based automation and validated using case studies.	1	1	2	4	8

Table IX : Score for all research papers

References	Score	Total
(Rane & Dixit, 2019),,(Manral & Somani et al., 2019),(Stoyanova & Nikoloudakis et al., 2020),(Khan et al., 2021),(Douglas et al., 2021),(Wu et al., 2021),(Ahmed & Singh, 2023),(Simou et al., 2019),(Zhang et al., 2023),(Al-Rawi & Boutaba, 2020),(Xu et al., 2021),(Santra & Dasgupta, 2020),(Almeida et al., 2023),(Singh & Patel, 2022),(Alhassan et al., 2023),(Zhang & Chen, 2022)	8	14
(Pandi & Shah et al., 2020),(Akter & Akther et al., 2020),(Balani & Varol, 2023),(Rahman & Alam, 2020),(Zou et al., 2019),(Karagiannis & Vergidis, 2021),(Hassan et al., 2023),(Rahim & Zafar, 2022),(Deebak & AL-Turjman, 2020),(Elmaghraby et al., 2021),(Rani et al., 2019),(Hemdan & Manjaiah, 2021),(Rahman et al., 2023)	7	10
(Brown & Glisson et al., 2022),(Achar & Khan, 2021),(Fernando, 2021) ,(Adeyeye et al., 2024),(Bernardini et al., 2022),(Montasari & Hill, 2024),(Pichan et al., 2018),(Ahmed et al., 2024),(Hossain & Rahman, 2022),(Prakash & Williams et al., 2022),(Patel & Kumar, 2024)	6	11
(Rakha, 2024),(Yassin & Abdollah et al., 2020),(Subramanian & Jeyaraj, 2018),(Akter & Rahman, 2024),(Kalaiarsan & Selvan, 2023),(Alenezi, 2024),(Baldwin et al., 2023),(Ali & Memon et al., 2020),(Cinar & Bharadiya, 2023),(Neware & Khan, 2020),(Liu et al., 2019),(Abiodun & Alawida et al., 2022)	5	12

After evaluating the papers based on factors such as relevance to the research questions, methodological rigor, and the impact of the findings, 14 papers scored 8, indicating a high level of quality and significant contributions to the cloud forensics domain. These papers are considered to have strong methodologies, comprehensive analyses, and a high degree of relevance to the research questions. 12 papers scored 7, which points out the good quality and well-structured methodologies with relevant findings; however, minor limitations identified. 11 papers were scored 6, insinuating while these studies contribute to the field, they must have some methodological weaknesses or a few limitations to the scope. Finally, 12 papers scored 5, indicating the need for these papers to provide useful insights but also depict gaps in methodology, analysis, or relevance, which needs improvement as shown in Table IX. This quality assessment helps in understanding the depth and reliability of the studies reviewed, guiding future research and development in the field of cloud forensics.

RQ#3) What are the primary forensic challenges encountered in cloud computing environments, and how do these challenges differ across various cloud service models (IaaS, PaaS, SaaS)?

Ans:

Cloud computing has fundamentally altered the way data is stored, processed, and accessed. The benefits of this technology include its scalability and cost efficiency, yet it presents digital forensic investigations with unique challenges. The forensic process, which involves evidence acquisition, preservation, analysis, and presentation, is more complex in a cloud environment compared to traditional systems. This complexity arises from the inherent characteristics of cloud computing: its distributed architecture, shared resources, and dynamic nature.

Each cloud service model—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—introduces unique challenges. For example, IaaS requires investigators to navigate virtualized environments, while SaaS relies heavily on service providers for evidence access. Addressing these challenges is crucial for maintaining the integrity of forensic investigations and ensuring that cloud computing environments remain secure and legally compliant as shown in Table X. Below is an analysis of key challenges based on existing literature, highlighting their importance and limitations.

1. **Multi-tenancy Issues:**

In cloud environments, there are many tenants on the same infrastructure; hence, evidence cannot be differentiated and isolated as belonging to one entity. It becomes contaminated with other tenants, and there are concerns about privacy and integrity in data. Forensic investigators can collect data that belongs to another tenant, thus violating legal and ethical standards, as reported by Ahmed et al. (2023).

2. **Data Volatility:**

Because of the dynamic nature of cloud systems, data can be modified or deleted very quickly. Such changes tend to complicate the process of preserving the evidence since traditional methods fail to capture the changes in real time. In cloud environments for example, forensic investigators face a lot of challenges in developing reliable snapshots of volatile data (Khan & Ali, 2024).

3. **Jurisdictional Barriers:**

Most data stored in the cloud is scattered across various geographies, hence falling under multiple legal jurisdictions. This makes jurisdictional barriers immense for investigators looking to access the data legally. For instance, it may take months to seek permission to retrieve data stored on a server located in another country (Patel & Kumar, 2024).

4. **Lack of Standardization:**

There is no standard of how forensic investigations are conducted in the cloud. Variability results in inconsistent practice and may also have an effect on the admissibility of evidence in court. Forensic teams have to operate under varying protocols set by the cloud providers, which further complicates their job (Park & Kim et al., 2018).

5. **Vendor Dependency:**

Cloud service providers hold critical data, such as logs and metadata, which are very important in forensic investigations. However, the forensic teams depend on the willingness of these vendors, who might not allow access to their information because of proprietary concerns or even their privacy policies (Zhang et al., 2023).

6. **Encryption Complexities:**

While encryption is a necessity for securing cloud data, it poses significant challenges to forensic investigations. Forensic teams often find it difficult to decrypt data without compromising its integrity, especially when dealing with advanced encryption algorithms (Santra & Dasgupta, 2020).

Table X: Primary forensic challenges

Author (in-text Citation)	**Challenges**	**Importance**	**Limitation**
(Ahmed et al., 2023(	Multi-tenancy Issues	Ensures evidence integrity by isolating data from shared environments.	Difficulty in isolating data without impacting other tenants.
(Khan & Ali, 2024)	Data Volatility	Highlights the need for real-time forensic mechanisms.	Frequent modifications and deletions make evidence preservation unreliable.
(Patel & Kumar, 2024)	Jurisdictional Barriers	Addresses legal compliance and cross-border investigation issues.	Complexities in obtaining legal access to data stored across multiple jurisdictions.
(Park & Kim et al., 2018)	Lack of Standardization	Advocates for consistent forensic practices across cloud systems.	Variability in standards leads to inconsistent evidence handling procedures.
(Zhang et al., 2023)	Vendor Dependency	Stresses the role of cloud providers in facilitating forensic investigations.	Limited access to proprietary logs and restricted investigator autonomy.

(Santra & Dasgupta, 2020)	Encryption Complexities	Emphasizes the importance of encryption in protecting data and challenges forensic decryption.	Strong encryption mechanisms create barriers to accessing critical evidence.

RQ#4) What techniques and tools have been proposed or implemented to address forensic challenges in cloud computing, and how effective are they in real-world scenarios?

Cloud computing is uniquely challenging in the forensic area. Data volatility, multi-tenancy, jurisdictional complexity, and encryption barriers are a few of these unique challenges. Specialized techniques and tools for these specific needs in cloud environments have been developed by researchers. Some of the notable ones include blockchain-based solutions for ensuring integrity in evidence, tenant isolation frameworks to manage multi-tenant setups, AI-driven tools to enhance evidence analysis, and snapshot-based methods to capture volatile data.

Each technique or tool focuses on specific forensic gaps, like traceability of evidence, management of access to encrypted data, or streamlining the investigative process as shown in Table XI. However, their real-world effectiveness varies depending on scalability, adaptability to cloud platforms, and compliance with legal and ethical standards. In controlled scenarios, these solutions appear promising, but their implementation in dynamic, real-world cloud ecosystems often reveals limitations that warrant further research and development.

1. **Blockchain for Evidence Management (Ahmed & Khan et al., 2023):**

Blockchain technology guarantees a tamper-proof system while maintaining the integrity of digital evidence. It generates an immutable ledger, which indicates that every piece of action concerning the evidence should be traceable and secure. For instance, in a forensic investigation, the blockchain can capture the entire chain of custody concerning the evidence against unauthorized alterations, but its huge computational cost raises issues with potential scalability when large datasets are present.

2. **Tenant Isolation Frameworks (Khan & Ali, 2024):**

Multi-tenancy in cloud environments complicates the separation of data from different users. Tenant isolation frameworks aim at segregating data to prevent contamination, which is very important in ensuring the admissibility of evidence. In static setups, these frameworks have been effective but are challenged by dynamic and large-scale cloud systems where tenant configurations frequently change.

3. **AI-Driven Evidence Analysis (Patel & Kumar, 2024):**

Artificial intelligence greatly enhances forensic investigations by automating evidence extraction and processing. For example, AI algorithms might quickly analyze large amounts of data, identifying patterns or Distinctive features that might be relevant to an investigation. However, AI requires significant computational resources and high-quality training datasets to deliver accurate results.

4. **Snapshot-Based Analysis (Zhang et al., 2023):**

Virtual machine snapshots capture the state of a system at a certain point in time, preserving volatile data that would otherwise be lost. This method is very helpful in investigating transient events in cloud systems. However, the intervals of the snapshots may lead to missing real-time changes, leaving gaps in the evidence.

5. **Encryption Decryption Tools (Santra & Dasgupta, 2020):**

Encryption protects the data in the cloud from unauthorized access but raises problems for forensic investigation. Custom decryption tools are provided to the investigators so that they can decrypt the encrypted data without damaging its integrity. Strong encryption mechanisms can sometimes delay or even make impossible the decryption process.

6. **Forensic-Enabled Cloud Services (Park & Kim et al., 2018):**

Proactive embedding of forensic capabilities in cloud services aids in dealing with challenges like volatility of data and multi-tenancy. For instance, readiness frameworks implemented directly into the product help evidence collection and analysis quickly. However, such tools are dependent on the goodwill of cloud service providers and are not applied universally.

Table XI: Techniques and Tools in Cloud Forensics

Author (in-text Citation)	Techniques & Tools	Importance	Limitation
(Ahmed & Khan et al., 2023)	Blockchain for Evidence Management	Ensures data integrity and maintains an immutable chain of custody.	High computational cost and scalability issues for large datasets.
(Khan & Ali, 2024)	Tenant Isolation Frameworks	Prevents data contamination in multi-tenant cloud environments.	Limited applicability in dynamic and large-scale cloud systems.
(Patel & Kumar, 2024)	AI-Driven Evidence Analysis	Speeds up evidence processing and improves accuracy in large datasets.	Requires significant computational resources and training data.
(Zhang et al., 2023)	Snapshot-Based Analysis	Captures volatile data reliably for forensic investigations.	May miss real-time changes in data during snapshot intervals.
(Santra & Dasgupta, 2020)	Encryption Decryption Tools	Enables access to encrypted data without compromising integrity.	Strong encryption mechanisms can delay or obstruct investigations.
(Park & Kim et al., 2018)	Forensic-Enabled Cloud Services	Proactively integrates forensic readiness into cloud infrastructures.	Relies on provider cooperation and lacks universal adoption across platforms.

RQ#5)How does the dynamic and distributed nature of cloud computing impact the acquisition, preservation, and analysis of digital evidence in forensic investigations?

The dynamic and distinguished architecture of cloud computing has transform data management and processing by offering scalability, cost-efficiency, and accessibility. However, this very nature introduces significant complexities in the forensic investigation process, particularly in the collection, preservation, and evaluation of digital evidence. The dynamic nature of cloud computing refers to the constant creation, modification, and deletion of data, which can occur across multiple geographic locations and systems in real time. Meanwhile, its dispersed nature suggests that data might be held in splintered fragments across different servers, usually under different jurisdictions and held by third-party cloud providers.

These characteristics pose unique challenges for forensic investigators. Data acquisition becomes difficult due to its transient state and dependency on cloud service providers for access. Preservation is further complicated by data volatility and multi-tenancy, where evidence can inadvertently be overwritten or lost. Analysis is hindered by encryption, limited visibility into proprietary cloud infrastructure, and the sheer volume of data involved. Advanced tools, protocols, and legal frameworks are needed to address these issues as shown in Table XII. Below, we discuss key impacts, supported by literature, summarized in a structured manner to highlight their importance and limitations.

1. **Real-Time Data Volatility (Ahmed & Khan et al., 2023):**

Cloud systems continuously generate and remove data, and it is a challenge for the investigators to acquire stable evidence. For instance, log files can be overwritten or purged before the investigators have access to them, which could create gaps in the evidence chain. This volatility requires real-time evidence acquisition tools to ensure that the data will be reliable.

2. **Distributed Storage and Jurisdictional Barriers (Khan & Ali, 2024):**

Data in cloud environments is usually scattered across different regions in the geographical location, meaning it is distributed and exposed to various legal and regulatory frameworks. For example, to access data in a foreign country, jurisdictional processes would be involved and thus complex to undertake. It thus challenges efficiency and timeliness in evidence acquisition.

3. **Multi-Tenancy Challenges (Patel & Kumar, 2024):**
Shared resources in multi-tenant environments can lead to evidence contamination because the data of different users is often intermingled. Isolating specific tenant data without affecting others requires precise technical solutions and cooperation from the cloud provider.

4. **Encryption Complexities (Zhang et al., 2023):**
Advanced encryption techniques that are used to protect cloud data make analysis difficult. Although encryption ensures data security, it may hinder forensic investigations by limiting access to critical evidence. Decryption processes are usually time-consuming and resource-intensive.

5. **Volume of Data (Santra & Dasgupta, 2020):**
The scale of data in cloud environments can be overwhelming for traditional forensic tools and methodologies. It requires specialized big data analysis tools and efficient workflows to extract the relevant evidence in terabytes or petabytes of distributed data

6. **Dependence on Cloud Service Providers (Park & Kim et al., 2018):**
Forensic investigations mainly depend on the cloud providers, which provide them with access to infrastructure, logs, and metadata. This kind of dependency constrains the evidence control of the investigators and often leads to provider policies that create delays or less than complete access to data.

Table XII: Impact of Cloud Computing on Digital Evidence

Author (in-text Citation)	Impact	Importance	Limitation
(Ahmed & Khan et al., 2023)	Real-Time Data Volatility	Highlights the need for real-time evidence acquisition tools.	Data may be overwritten or purged before access is granted.
(Khan & Ali, 2024)	Distributed Storage	Ensures coverage of evidence stored across multiple geographic regions.	Complex jurisdictional processes delay data access.
(Patel & Kumar, 2024)	Multi-Tenancy Challenges	Prevents contamination of evidence by isolating tenant-specific data.	Requires precise isolation techniques and cooperation from cloud providers.
(Zhang et al., 2023)	Encryption Complexities	Ensures data security but challenges forensic access.	Time-consuming decryption processes obstruct timely investigations.
(Santra & Dasgupta, 2020)	Volume of Data	Stresses the need for scalable tools to handle large datasets.	Traditional forensic tools are inadequate for analyzing massive volumes of data.
(Park & Kim et al., 2018)	Dependence on Cloud Providers	Ensures access to critical evidence through provider cooperation.	Limits investigator control and may result in delays or incomplete evidence.

Taxonomy:

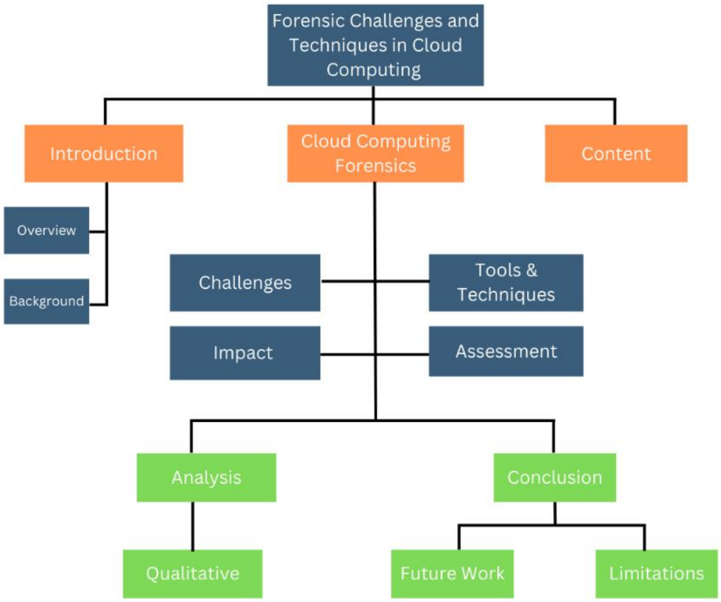


Fig VIII: Taxonomy

Conclusion

This SLR analyzed the forensic challenges and techniques that occur in cloud computing environments based on the nature of the cloud systems as dynamic and distributed. From the critical analysis of 52 high-quality research papers, the following general findings were concluded. Among them, data volatility, multi-tenancy, jurisdictional barriers, and encryption complexities are some of the key challenges that are amplified in cloud environments due to the shared nature of resources and the global distribution of data. In response to these challenges, a variety of forensic tools and techniques have been proposed, including blockchain-based evidence management systems, AI-driven tools for evidence analysis, tenant isolation frameworks, and snapshot-based methods for capturing volatile data. Although these tools have proved to be successful in a controlled setup, their utility beyond the lab is still very minimal, and significant challenges include data privacy, cooperation of service providers, and urgent acquisition of evidence through real-time means. However, significantly sized gaps in standard methodologies exist, chief among them being the absence of uniformity in forensic processes and the need for comprehensive forensic readiness across cloud levels. This review contributes valuable insights into the current state of cloud forensics research and lays the groundwork for future advancements in this field.

Future Work

This review has thus been able to outline the forensic challenges and techniques within cloud computing comprehensively, with several areas yet to be fully explored. Some of the future research areas would include developing standard forensic methodologies applicable universally in IaaS, PaaS, and SaaS-based cloud service models. Standardization is of the utmost importance for establishing consistency and reliability in cloud forensic investigation and, subsequently enhancing the admissibility of digital evidence in legal court. The dynamic as well as rapidly evolving nature of environments demands real-time forensic tools that efficiently capture and preserve volatile data. Future work would be to provide high-performance, lightweight tools that really minimize latency in evidence collection as well as processing. Another significant direction for research involves the development of robust legal and regulatory frameworks to deal with jurisdictional issues associated with cloud forensics, especially in the context of cross-border investigations. Such frameworks could help streamline the forensic process by harmonizing access to data across jurisdictions. Integration of AI and blockchain technologies with cloud forensics is still an underdeveloped area. Future studies could explore how these technologies can be combined to build a more secure, scalable, and efficient forensic infrastructure in the cloud. Finally, fostering stronger cooperation between cloud service providers and forensic investigators is crucial. Future research could aim to develop industry-wide standards for forensic readiness, ensuring that providers support and facilitate forensic investigations through clear guidelines and protocols. By addressing these challenges, future research in cloud forensics will enhance forensic capabilities, improve the integrity of cloud-based investigations, and lay the foundation for more effective and reliable forensic practices in the cloud computing environment.

REFERENCES:

Abiodun, O. I., Alawida, M., Omolara, A. E., & Alabdulatif, A. (2022). Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey. *Journal of King Saud University-Computer and Information Sciences*, *34*(10), 10217-10245.

Achar, S. (2022). Cloud computing forensics. *International Journal of Computer Engineering and Technology*, *13*(3), 1-10.

Akbar, H., Zubair, M., & Malik, M. S. (2023). The security issues and challenges in cloud computing. *International Journal for Electronic Crime Investigation*, 7(1), 13-32.

Akter, O., Akther, A., Uddin, M. A., & Islam, M. M. (2020). Cloud forensics: Challenges and blockchain based solutions. *International Journal of Wireless and Microwave Technologies*, *10*(5), 1-12.

Akter, O., Akther, A., Uddin, M. A., & Islam, M. M. (2020). Cloud forensics: Challenges and blockchain based solutions. *International Journal of Wireless and Microwave Technologies*, *10*(5), 1-12.

Akter, S. S., & Rahman, M. S. (2024). Cloud Forensic: Issues, Challenges, and Solution Models. In *A Practical Guide on Security and Privacy in Cyber-Physical Systems: Foundations, Applications and Limitations* (pp. 113-152).

Akter, S. S., & Rahman, M. S. (2024). Cloud Forensic: Issues, Challenges, and Solution Models. In *A Practical Guide on Security and Privacy in Cyber-Physical Systems: Foundations, Applications and Limitations* (pp. 113-152).

Alenezi, A., Atlam, H. F., & Wills, G. B. (2019). Experts reviews of a cloud forensic readiness framework for organizations. *Journal of Cloud Computing*, *8*, 1-14.

Ali, M. I., Kaur, S., Khamparia, A., Gupta, D., Kumar, S., Khanna, A., & Al-Turjman, F. (2020). Security challenges and cyber forensic ecosystem in IOT driven BYOD environment. *IEEE Access*, *8*, 172770-172782.

Ali, S. A., Memon, S., & Sahito, F. (2018, August). Challenges and solutions in cloud forensics. In *Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing* (pp. 6-10).

Al-mugern, R., Othman, S. H., Al-Dhaqm, A., & Ali, A. (2024). A Cloud Forensics Framework to Identify, Gather, and Analyze Cloud Computing Incidents. *Engineering, Technology & Applied Science Research*, *14*(3), 14483-14491.

Balani, Z., & Varol, H. (2020, June). Cloud computing security challenges and threats. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-4). IEEE.

Baldwin, J., Alhawi, O. M., Shaughnessy, S., Akinbi, A., & Dehghantanha, A. (2018). Emerging from the cloud: A bibliometric analysis of cloud forensics studies. *Cyber threat intelligence*, 311-331.

Brown, A. J., Glisson, W. B., Andel, T. R., & Choo, K. K. R. (2018). Cloud forecasting: Legal visibility issues in saturated environments. *Computer Law & Security Review*, *34*(6), 1278-1290.

Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., ... & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*, *10*, 25464-25493.

Chen, L., Takabi, H., & Le-Khac, N. A. (Eds.). (2019). *Security, privacy, and digital forensics in the cloud*. John Wiley & Sons.

Cinar, B., & Bharadiya, J. P. (2023). Cloud computing forensics; challenges and future perspectives: A review. *Asian Journal of Research in Computer Science*, *16*(1), 1-14.

Deebak, B. D., & Fadi, A. T. (2021). Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing. *Future generation computer systems*, *116*, 406-425.

Dixit, V., & Kaur, D. (2024). Secure and Efficient Outsourced Computation in Cloud Computing Environments. *Journal of Software Engineering and Applications*, *17*(9), 750-762.

Fakhouri, H. N., AlSharaiah, M. A., Alkalaileh, M., & Dweikat, F. F. (2024, February). Overview of Challenges Faced by Digital Forensic. In *2024 2nd International Conference on Cyber Resilience (ICCR)* (pp. 1-8). IEEE.

Fernando, V. (2021, April). Cyber forensics tools: A review on mechanism and emerging challenges. In *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-7). IEEE.

Ganesh, N. G., Venkatesh, N. M., & Prasad, D. V. V. (2022). A systematic literature review on forensics in cloud, IoT, AI & blockchain. *Illumination of Artificial Intelligence in Cybersecurity and Forensics*, 197-229.

Hemdan, E. E. D., & Manjaiah, D. H. (2021). An efficient digital forensic model for cybercrimes investigation in cloud computing. *Multimedia Tools and Applications*, *80*, 14255-14282.

Herman, M., Herman, M., Iorga, M., Salim, A. M., Jackson, R. H., Hurst, M. R., ... & Sardinas, R. (2020). *Nist cloud computing forensic science challenges*. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.

Islam, M. J., Mahin, M., Khatun, A., Roy, S., Kabir, S., & Debnath, B. C. (2019). A comprehensive data security and forensic investigation framework for cloud-iot ecosystem. *GUB J. Sci. Eng*, *4*(1), 1-12.

Kalaiarsan, M., & Selvan, P. T. (2024). Assessing the Role of Cloud Computing in Ransomware Attacks and Digital Forensics Investigations. *SPAST Reports*, *1*(3).

Karagiannis, C., & Vergidis, K. (2021). Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal. *Information*, *12*(5), 181.

Kebande, V. R., & Venter, H. S. (2018). Novel digital forensic readiness technique in the cloud environment. *Australian Journal of Forensic Sciences*, *50*(5), 552-591.

Kebande, V. R., & Venter, H. S. (2018). On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges. *Australian Journal of Forensic Sciences*, *50*(2), 209-238.

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

Malik, A. W., Bhatti, D. S., Park, T. J., Ishtiaq, H. U., Ryou, J. C., & Kim, K. I. (2024). Cloud digital forensics: Beyond tools, techniques, and challenges. *Sensors*, *24*(2), 433.

Manral, B., Somani, G., Choo, K. K. R., Conti, M., & Gaur, M. S. (2019). A systematic survey on cloud forensics challenges, solutions, and future directions. *ACM Computing Surveys (CSUR)*, *52*(6), 1-38.

Montasari, R., & Hill, R. (2019, January). Next-generation digital forensics: Challenges and future paradigms. In *2019 IEEE 12th International conference on global security, safety and sustainability (ICGS3)* (pp. 205-212). IEEE.

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

Neware, R., & Khan, A. (2018, March). Cloud computing digital forensic challenges. In *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1090-1092). IEEE.

Pandi, G. S., Shah, S., & Wandra, K. H. (2020). Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation. *Procedia Computer Science*, *167*, 163-173.

Park, S., Kim, Y., Park, G., Na, O., & Chang, H. (2018). Research on digital forensic readiness design in a cloud computing-based smart work environment. *Sustainability*, *10*(4), 1203.

Pichan, A., Lazarescu, M., & Soh, S. T. (2018). Towards a practical cloud forensics logging framework. *Journal of information security and applications*, *42*, 18-28.

Pourvahab, M., & Ekbatanifard, G. (2019). Digital forensics architecture for evidence collection and provenance preservation in iaas cloud environment using sdn and blockchain technology. *IEEE Access*, *7*, 153349-153364.

Prakash, V., Williams, A., Garg, L., Barik, P., & Dhanaraj, R. K. (2022). Cloud-based framework for performing digital forensic investigations. *International Journal of Wireless Information Networks*, *29*(4), 419-441.

Prakash, V., Williams, A., Garg, L., Savaglio, C., & Bawa, S. (2021). Cloud and edge computing-based computer forensics: Challenges and open problems. *Electronics*, *10*(11), 1229.

Purnaye, P., & Kulkarni, V. (2022). A comprehensive study of cloud forensics. *Archives of Computational Methods in Engineering*, *29*(1), 33-46.

Rane, S., & Dixit, A. (2019). BlockSLaaS: Blockchain assisted secure logging-as-a-service for cloud forensics. In *Security and Privacy: Second ISEA International Conference, ISEA-ISAP 2018, Jaipur, India, January, 9–11, 2019, Revised Selected Papers 2* (pp. 77-88). Springer Singapore.

Rani, D. R., & Geethakumari, G. (2020). Secure data transmission and detection of anti-forensic attacks in cloud environment using MECC and DLMNN. *Computer Communications*, *150*, 799-810.

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

Sachdeva, S., & Ali, A. (2022). Machine learning with digital forensics for attack classification in cloud network environment. *International Journal of System Assurance Engineering and Management*, *13*(Suppl 1), 156-165.

Santra, P., Roy, A., & Majumder, K. (2018). A Comparative analysis of cloud forensic techniques in IaaS. In *Advances in Computer and Computational Sciences: Proceedings of ICCCCS 2016, Volume 2* (pp. 207-215). Springer Singapore.

Simou, S., Kalloniatis, C., Gritzalis, S., & Katos, V. (2019). A framework for designing cloud forensic-enabled services (CFeS). *Requirements Engineering*, *24*, 403-430.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.

Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers & Electrical Engineering*, *71*, 28-42.

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), 9493-9532.

Thabit, F., Alhomdy, S. A. H., Alahdal, A., & Jagtap, S. B. (2020). Exploration of security challenges in cloud computing: Issues, threats, and attacks with their alleviating techniques. *Journal of Information and Computational Science*, *12*(10).

Williams, M., Emeteveke, I., Adeyeye, O. J., & Emehin, O. *Enhancing Data Forensics through Edge Computing in IoT Environments*.

Williams, M., Emeteveke, I., Adeyeye, O. J., & Emehin, O. *Enhancing Data Forensics through Edge Computing in IoT Environments*.

Yassin, W., Abdollah, M. F., Ahmad, R., Yunos, Z., & Ariffin, A. (2020). Cloud forensic challenges and recommendations: A review. *OIC-CERT Journal of Cyber Security*, *2*(1), 19-29.

Zou, D., Zhao, J., Li, W., Wu, Y., Qiang, W., Jin, H., ... & Yang, Y. (2018). A multigranularity forensics and analysis method on privacy leakage in cloud environment. *IEEE Internet of Things Journal*, *6*(2), 1484-1494.