IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13245

An Organized Retrospect of Cloud Forensic

Juber Mirza[1], Manish Sharma[2], Rupali Dave[3]

Assistant Professor, Computer Science and Engineering, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, India[1]

Assistant Professor, Computer Science and Engineering, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, India[2]

Assistant Professor, Computer Science and Engineering, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, India[3]

Abstract: Cloud computing has revolutionized the way data is stored, processed and accessed, providing unprecedented scalability and flexibility to businesses and individuals alike. However, the inherent complexity and distributed nature of cloud environments also introduce new challenges for digital forensics investigations. This paper explores the emerging field of cloud forensic techniques, methodologies and tools tailored to investigate incidents in cloud environments. By reviewing existing literature and methodologies, we identify key challenges such as data privacy, evidence preservation and chain of custody maintenance. We also propose a framework for conducting cloud forensic investigations, integrating traditional forensic principles with cloud-specific considerations. Through case studies and experiments, we demonstrate the effectiveness and limitations of current cloud forensic approaches, paving the way for future research and development in this critical area of cybersecurity. Ultimately, this paper contributes to the advancement of knowledge in cloud forensic research by providing a comprehensive understanding of the challenges, methodologies and tools necessary to investigate incidents within cloud computing environments. By addressing these challenges and fostering interdisciplinary collaboration, we aim to enhance the effectiveness and reliability of cloud forensic investigations, thereby ensuring the security and trustworthiness of cloud-based services in an increasingly digital world.

Keywords: Digital forensic, Cloud forensic, Cloud computing, Cybersecurity.

I. INTRODUCTION

Cloud computing has emerged as a dominant paradigm in the modern era of computing, offering unparalleled scalability, flexibility and accessibility to individuals and organizations alike. By leveraging remote servers hosted on the internet to store, manage and process data, cloud computing has revolutionized the way information technology services are delivered, enabling businesses to achieve unprecedented levels of efficiency and innovation. However, this paradigm shift towards cloud-based solutions has also introduced new challenges in terms of security, privacy and digital forensic investigations. Traditionally, digital forensic investigations have been conducted within the confines of on-premises IT infrastructures, where investigators have direct access to physical devices and storage media. However, the distributed and virtualized nature of cloud environments presents unique challenges to traditional forensic methodologies[3]. In cloud computing, data is often dispersed across geographically distributed servers, shared among multiple users and dynamically allocated and reallocated based on demand. Consequently, investigating incidents such as data breaches, unauthorized access, or malicious activities within cloud environments requires specialized techniques, methodologies and tools tailored to the unique characteristics of cloud computing[19].

The field of cloud forensic research has emerged in response to these challenges, aiming to develop effective strategies and technologies for conducting investigations in cloud environments. Cloud forensic encompasses a wide range of activities, including evidence acquisition, preservation, analysis and presentation, adapted to the distributed and dynamic nature of cloud infrastructures. Key challenges in cloud forensic investigations include ensuring the integrity and authenticity of digital evidence, preserving chain of custody across multiple jurisdictions and service providers and navigating complex legal and regulatory frameworks governing cloud data.

This research paper seeks to contribute to the burgeoning field of cloud forensic science by providing a comprehensive overview of the challenges, methodologies and tools relevant to investigating incidents in cloud environments. Through an extensive review of existing literature and case studies, we aim to identify the gaps and limitations in current cloud forensic practices and propose novel solutions to address these challenges. figure 1 shows detailed process of cloud forensics anatomy.

The remainder of this paper is organized as follows: Section II provides a comprehensive review of the existing literature on cloud forensic research, including key concepts, challenges and methodologies. Section III presents why we use cloud forensic in digital landscape.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13245

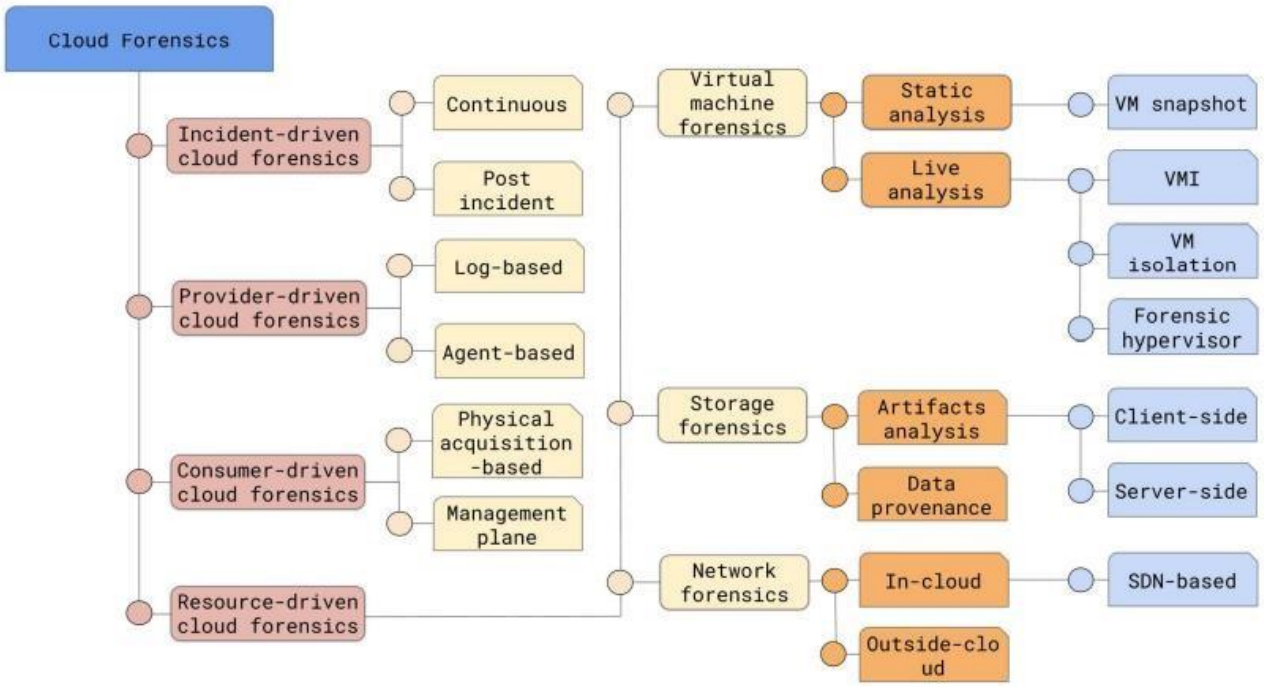

Fig. 1 Cloud Forensics anatomy

Section IV discusses the process of cloud forensic investigation Section V presents related work like algorithms, techniques and tools. Finally, Section 6 concludes the paper with a summary of key findings, implications for future research and recommendations for practitioners in the field of cloud forensic science.

II. LITERATURE REVIEW

Cloud forensics is an emerging field that addresses the challenges of collecting, preserving and analysing digital evidence in cloud computing environments. A comprehensive literature review provides insight into the current state of research, identifies gaps in knowledge and guides future research directions. Here's a detailed overview of the literature on cloud forensics for research work writing:

Foundational Concepts and Definitions: Researchers have established foundational concepts and definitions in cloud forensics, clarifying terminology and outlining the scope of the field. Early works by authors such as Reedy and Spafford (2009) and Ruan et al. (2010) provide an introduction to cloud forensics principles and methodologies.

Taxonomies and Frameworks: Taxonomies and frameworks are developed to categorize cloud forensic challenges and methodologies. Al Mutawa et al. (2016) proposed a taxonomy of cloud forensic challenges, categorizing them into dimensions such as data location, multi-tenancy and service models. Slay et al. (2017) introduced a conceptual framework for cloud forensic readiness, outlining key components and processes.

Challenges and Solutions: Literature reviews explore the challenges and solutions in cloud forensics investigations. Martini et al. (2014) identified challenges related to evidence acquisition, preservation, and analysis in cloud environments. Raghavan et al. (2018) discussed legal and regulatory challenges in cloud forensics and proposed solutions for ensuring compliance.

Forensic Techniques and Tools: Researchers have developed forensic techniques and tools tailored to cloud environments. Carthy et al. (2019) introduced CloudFence, a tool for acquiring and analysing evidence from cloud storage services. Peer et al. (2020) proposed a forensic analysis framework for virtualized cloud environments, leveraging memory forensics and network analysis techniques.

Case Studies and Empirical Studies: Case studies and empirical studies provide insights into real-world applications of cloud forensics techniques. Khan et al. (2020) conducted experiments to evaluate forensic tools' effectiveness in extracting evidence from cloud-based storage services. Yamin et al. (2017) analysed challenges and limitations in multi-tenant cloud forensic investigations through simulated scenarios.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13245

Legal and Ethical Considerations: Legal and ethical considerations are integral to cloud forensics investigations. Martini et al. (2016) examined jurisdictional challenges and data privacy laws impacting cloud forensic investigations. Authors such as Martini and Choo (2015) and Hayes et al. (2017) discussed ethical considerations and guidelines for conducting cloud forensics research.

III. WHY CLOUD FORENSIC?

Cloud computing has become the backbone of modern digital infrastructure, offering unparalleled scalability, flexibility, and cost-effectiveness to organizations across various industries. However, the widespread adoption of cloud technologies has also given rise to new challenges in terms of security, privacy and compliance. As organizations increasingly rely on cloud services to store and process sensitive data, the need for robust cloud forensic capabilities has become paramount. This section outlines the pressing need for cloud forensic research and highlights key reasons why it is essential in today's digital landscape.

a. **Complexity and Distributed Nature of Cloud Environments**: Cloud infrastructures are inherently complex and distributed, with data being dispersed across geographically diverse servers and shared among multiple users[42]. This distributed nature presents significant challenges for traditional forensic methodologies, which are designed for on-premises environments with direct access to physical devices. Investigating incidents such as data breaches or unauthorized access in cloud environments requires specialized techniques and tools capable of navigating this complexity and capturing digital evidence effectively.

b. **Dynamic Resource Allocation and Multi-Tenancy**: Cloud environments operate on a model of dynamic resource allocation, where computing resources are provisioned and deprovisioned based on demand. Additionally, cloud services often operate on a multi-tenant architecture, where multiple users share the same underlying infrastructure. These dynamic and multi-tenant characteristics pose challenges for forensic investigators in terms of isolating and preserving digital evidence associated with specific users or instances. Furthermore, the co-mingling of data from multiple tenants complicates the process of attribution and accountability in the event of a security incident[46].

c. **Data Privacy and Compliance Requirements**: Data privacy and compliance regulations impose stringent requirements on organizations regarding the protection and handling of sensitive data, especially when it is stored or processed in cloud environments[12]. Forensic investigations in cloud computing must adhere to these regulations while ensuring the confidentiality, integrity and availability of digital evidence. Moreover, the cross-border nature of cloud computing introduces additional complexities related to jurisdictional differences and legal frameworks, necessitating careful consideration of legal and ethical considerations in cloud forensic practices.

d. **Rapid Evolution of Cloud Technologies:** Cloud technologies are constantly evolving, with new services, features and deployment models being introduced regularly. As cloud infrastructures continue to evolve, so too must the techniques and methodologies used in cloud forensic investigations. Research efforts in cloud forensic science are essential to keep pace with these rapid advancements, ensuring that investigators have the necessary tools and knowledge to effectively address emerging threats and challenges in cloud computing[10].

e. **Enhancing Incident Response and Security Posture:** Effective cloud forensic capabilities are essential for organizations to respond promptly and effectively to security incidents, minimize the impact of breaches and mitigate future risks. By investing in cloud forensic research, organizations can improve their incident response capabilities, strengthen their security posture and enhance overall resilience against cyber threats in cloud environments.

IV. PROCESS OF CLOUD FORENSIC INVESTIGATION

Cloud forensic investigations involve a systematic approach to collecting, analysing and presenting digital evidence related to security incidents or unauthorized activities within cloud environments. This process is guided by established forensic principles adapted to the unique characteristics of cloud computing. This section outlines the key steps involved in the process of cloud forensic investigation.

Preparation and Planning: Before initiating a cloud forensic investigation, it is essential to develop a comprehensive plan outlining the objectives, scope, and resources required for the investigation. This includes identifying the type of cloud service (e.g., SaaS, PaaS, IaaS) involved, determining the legal and regulatory considerations and assessing the potential impact on business operations. Additionally, investigators should establish communication channels with relevant stakeholders, such as cloud service providers, legal teams and internal IT personnel, to facilitate coordination and cooperation throughout the investigation[18].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13245

Evidence Identification and Preservation: The first step in any forensic investigation is to identify and preserve digital evidence relevant to the case. In cloud environments, this involves identifying the types of data and artifacts that may contain evidence of the incident, such as log files, configuration settings, network traffic, and user activity logs. Specialized tools and techniques may be used to capture and preserve volatile data from running instances or virtual machines (VMs) without compromising their integrity. It is crucial to document the chain of custody and maintain the integrity of the evidence throughout the preservation process[1].

Evidence Collection and Acquisition: Once the relevant evidence has been identified and preserved, investigators proceed with collecting and acquiring the data from cloud storage repositories, virtual machines, network devices and other relevant sources. This may involve obtaining forensic copies of disk images, memory dumps, network captures and metadata associated with the cloud environment. Care should be taken to adhere to legal and regulatory requirements, obtain necessary permissions from cloud service providers, and minimize disruption to ongoing operations during the acquisition process[5].

Data Analysis and Examination: With the evidence collected, investigators proceed to analyse and examine the data to identify patterns, anomalies, and indicators of compromise. This may involve using forensic analysis tools and techniques to parse log files, reconstruct timelines of events, correlate disparate data sources and identify potential sources of intrusion or unauthorized access. Machine learning and data mining techniques may be employed to automate the analysis process and uncover hidden insights from large datasets[4]. Throughout this phase, investigators must maintain meticulous documentation of their findings and methodologies to ensure the reproducibility and validity of their conclusions.

Interpretation and Reconstruction: Once the data analysis is complete, investigators interpret the findings and reconstruct the sequence of events leading up to and during the security incident. This may involve developing hypotheses and scenarios based on the evidence collected, identifying potential motives and actors involved and assessing the impact of the incident on the organization's systems and data. Collaboration with subject matter experts, such as cybersecurity analysts, legal counsel and forensic specialists, may be necessary to validate interpretations and draw meaningful conclusions from the evidence[8].

Reporting and Documentation: The final step in the cloud forensic process is to prepare a comprehensive report documenting the findings, analysis and conclusions of the investigation. The report should provide a clear and concise overview of the incident, including a summary of the evidence collected, analysis performed and conclusions drawn. Additionally, it should include recommendations for remediation and mitigation measures to prevent similar incidents in the future. The report should be prepared in accordance with legal and regulatory requirements, ensuring that it is admissible as evidence in any legal proceedings that may arise from the incident[40].overall research strategy shown in figure 2.

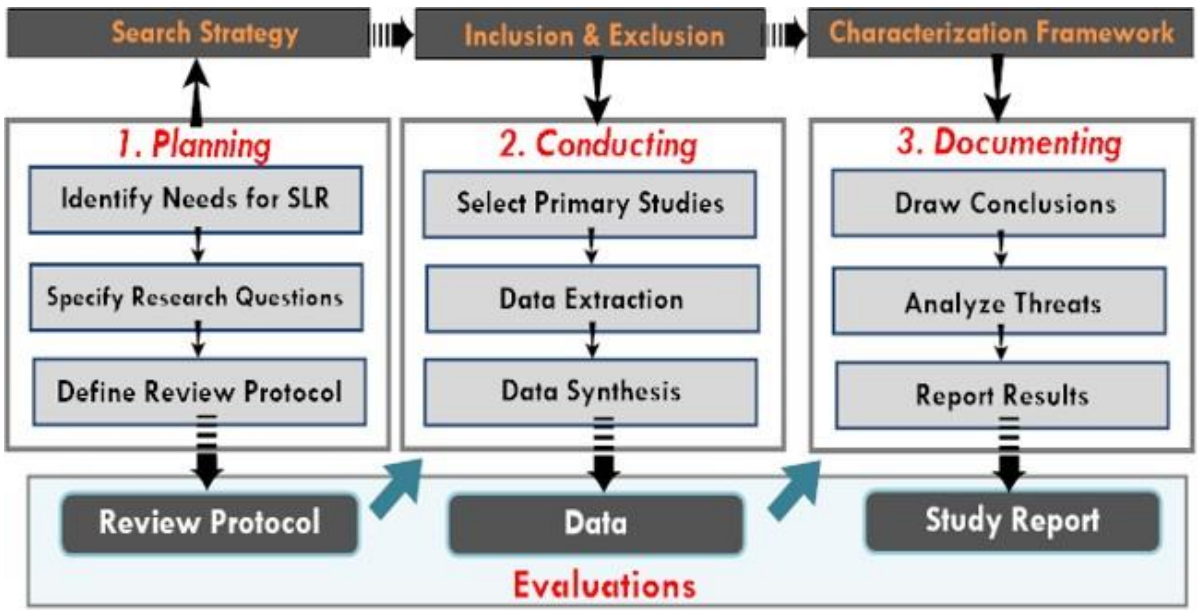

Fig. 2 Research Strategy

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13245

V. RELATED WORK: ALGORITHMS, TECHNIQUES AND TOOLS

Cloud forensic investigations in cloud computing environments typically involve a variety of algorithms and techniques for data acquisition, analysis and interpretation. Here we are discussed some key algorithms commonly used in cloud forensics environment:

Data Acquisition Algorithms:
Live Data Acquisition Algorithms: These algorithms are used to collect volatile data from live systems, such as memory dumps, process listings, network connections and open files. Examples include tools like Volatility for memory forensics and network sniffers for capturing network traffic.

Disk Imaging Algorithms: Algorithms for creating forensic disk images of cloud storage volumes, virtual machine disks, or physical disks. These algorithms ensure a bit-by-bit copy of the original storage device, preserving its integrity for analysis. Common imaging algorithms include dd (Disk Dump) and tools like FTK Imager or EnCase.

Data Analysis Algorithms:
File Carving Algorithms: These algorithms are used to recover deleted or fragmented files from disk images or storage volumes. File carving algorithms analyse the raw data to identify file headers, footers and signatures, reconstructing files based on these patterns. Examples include the Scalpel and Foremost tools.

Timeline Analysis Algorithms: Algorithms for creating timelines of system events and user activities based on forensic artifacts extracted from the collected data. Timeline analysis algorithms correlate timestamps and metadata to reconstruct a chronological sequence of events relevant to the investigation. Tools like Plaso (log2timeline) and Sleuth Kit/Autopsy provide support for timeline analysis.

Hashing Algorithms: Cryptographic hash algorithms such as MD5, SHA-1 and SHA-256 are used to calculate checksums of files and data blocks. Hashing algorithms are employed for data integrity verification, duplicate file identification and digital signature verification in cloud forensic investigations.

TABLE I :ANALYSIS OF EXISTING METHODOLOGIES

References	*Evidence Collection Techniques*	*Forensics Analysis*	*Framework Proposed*	*Implementation Details*	*AI/Machin e Learning*	*Trust Provenance*
Kao et.al		✓	✓	✓		✓
Povar et.al		✓	✓		✓	✓
M. Ahsan et.al	✓	✓		✓		
C. Federici et.al	✓	✓		✓	✓	✓
S. Almulla et.al		✓	✓	✓	✓	✓
S. S. Sampana et.al	✓	✓	✓			
Zawoad et.al	✓		✓			
R. Battistoni et.al	✓	✓		✓	✓	
E. Hemdan et.al				✓	✓	✓
Roussev et.al		✓		✓	✓	

Data Interpretation Algorithms: Metadata Analysis Algorithms: Algorithms for extracting and analysing metadata associated with files, documents and system objects. Metadata analysis algorithms reveal information such as file timestamps, file attributes, user permissions and file ownership, which can provide valuable insights into the context of the data.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024
DOI: 10.17148/IJARCCE.2024.13245

Pattern Recognition Algorithms: These algorithms are used to identify patterns of suspicious behaviour or anomalies in the forensic data. Pattern recognition algorithms may employ machine learning and statistical analysis techniques to detect unusual access patterns, network traffic anomalies, or malicious activity indicators.

Network Forensics Algorithms:
Packet Analysis Algorithms: Algorithms for analysing network traffic captures to identify and reconstruct communication sessions, extract transmitted data, and identify suspicious or malicious network activity. Packet analysis algorithms often involve protocols-specific parsers and pattern matching techniques.

Flow Analysis Algorithms: Algorithms for analysing flow data generated by network devices, such as NetFlow or Flow records. Flow analysis algorithms aggregate and analyse flow data to identify trends, anomalies and potential security incidents in network traffic. These algorithms are utilized in combination with specialized tools and methodologies to conduct effective forensic investigations in cloud computing environments. The selection of algorithms depends on the specific requirements of the investigation, the types of evidence available, and the goals of the forensic analysis.

Cloud forensic investigations rely on a variety of specialized tools and software applications to collect, analyze, and preserve digital evidence within cloud environments[19]. These tools facilitate the forensic process by providing capabilities for data acquisition, evidence preservation, analysis and reporting. Here is a detailed overview of the tools commonly used in cloud forensics, categorized based on their primary functionalities:

TABLE II: CLOUD FORENSIC TOOLS

Virtual Forensics Computing [21]	Forensic Image of a suspect is booted
Wireshark [35]	Captures network traffic between VM and the CSP
Microsoft Expression Encoder4 [25]	VM windows video recorder
FTK Imager [52]	Memory and disk images acquisition.
Encase Remote Agent [28]	Acquisition of Windows and Linux live system
FROST [34]	Digital forensics tools for the OpenStack cloud platform
Xen Access [24]	Xen VM introspection library (Hypervisor level)
Bon Fire [36]	An EU project enables operating a multi-site cloud-based facility on top of different infrastructure
	testbeds such as Emulab
Eucalyptus [51]	A software used to build Amazon Workstation (AWS) private and public cloud
Cloud Sim [52]	A solution to create large-scale cloud computing data center, virtual hosts, and capability of analysis for network traffic
OpenStack [54]	A project used to create various IaaS architectures such as storage, compute and network
Rack space [44]	Based on OpenStack and provides IaaS.

VI. CHALLENGES OF CLOUD FORENSIC INVESTIGATION

Chain of Custody and Evidence Preservation: Maintaining the integrity and chain of custody of digital evidence is challenging in cloud environments where data is constantly in flux and subject to dynamic changes. Investigators must implement robust mechanisms for preserving digital evidence, including capturing forensic images of virtual machines, documenting metadata associated with cloud resources and maintaining detailed logs of investigative actions. Ensuring the admissibility of digital evidence in legal proceedings requires meticulous documentation of the chain of custody and adherence to forensic best practices.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024
DOI: 10.17148/IJARCCE.2024.13245

Multi-Tenancy and Shared Resources: Cloud services often operate on a multi-tenant architecture, where multiple users share the same underlying infrastructure and resources. This shared environment introduces challenges in isolating and attributing malicious activities to specific users or instances. Investigative techniques must account for the potential impact of neighbouring tenants on the integrity and availability of digital evidence, as well as the risk of contamination or interference between concurrent investigations conducted on the same infrastructure[35].

Dynamic Resource Allocation and Volatility: Cloud environments operate on a model of dynamic resource allocation, where computing resources are provisioned and deprovisioned based on demand. This dynamic nature introduces volatility into forensic investigations, as evidence may be transient and ephemeral, requiring real-time capture and analysis techniques to preserve its integrity. Moreover, the scalability and elasticity of cloud services make it challenging to predict and control the behaviour of cloud resources during an investigation, necessitating adaptability and agility in forensic methodologies[47].

Legal and Jurisdictional Issues: Cloud forensic investigations often span multiple jurisdictions, each with its own legal and regulatory frameworks governing the collection, handling and disclosure of digital evidence. Investigators must navigate complex legal issues related to jurisdictional boundaries, data sovereignty and international cooperation, particularly in cases involving cross-border data transfers or multinational cloud service providers. Ensuring compliance with applicable laws and regulations while conducting investigations in cloud environments requires careful consideration of legal and ethical considerations[11].

Data Location and Ownership: In cloud environments, data is often distributed across geographically diverse servers, making it challenging for investigators to ascertain the physical location of data relevant to the investigation. Additionally, cloud service providers may use data replication and redundancy techniques to improve reliability and availability, further complicating efforts to identify the authoritative source of data. Moreover, determining ownership and control of data stored in multi-tenant cloud environments can be challenging, as data from multiple users may be co-mingled on the same infrastructure[21].

Data Privacy and Confidentiality: Cloud forensic investigations must navigate complex data privacy regulations and contractual agreements governing the handling and disclosure of sensitive information stored in cloud environments. Investigators must ensure that their actions comply with applicable legal and regulatory requirements, such as data protection laws (e.g., GDPR, HIPAA) and contractual obligations outlined in service level agreements (SLAs) with cloud service providers. This includes obtaining necessary permissions and consent for accessing and analysing data, as well as safeguarding the confidentiality and privacy of sensitive information throughout the investigation process[33].

VII. CONCLUSION

Cloud computing has transformed the landscape of data storage and processing, offering unprecedented scalability, flexibility and accessibility to organizations worldwide. However, this shift to the cloud has introduced new challenges for digital forensic investigations. Throughout this research paper we have explored the complexities, advancements and future directions of cloud forensic investigations, aiming to shed light on this critical aspect of modern cybersecurity.

Challenges and Complexities: The migration of data and applications to cloud environments introduces complexities that traditional forensic methodologies may struggle to address. Challenges such as multi-tenancy, data sovereignty and shared responsibility models require innovative approaches to evidence collection, analysis, and attribution.

Emerging Technologies: Advances in technology, particularly in artificial intelligence, machine learning and cloud-native forensic tools, offer promising solutions to enhance the capabilities of cloud forensic investigations. These technologies enable automated evidence analysis, real-time threat detection and predictive analytics, empowering investigators to adapt to the dynamic nature of cloud environments.

Standardization and Collaboration: Standardizing procedures, methodologies and tools is essential for ensuring consistency, reliability and interoperability in cloud forensic investigations. Collaborative efforts between academia, industry, law enforcement and regulatory agencies are crucial for advancing cloud forensic capabilities and fostering innovation in the field.

Education and Training: Education and training play a pivotal role in preparing forensic practitioners to navigate the complexities of cloud environments effectively. Developing standardized curricula, certification programs and continuing education opportunities is essential to equip professionals with the knowledge, skills and competencies required to conduct rigorous investigations in cloud computing environments.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13245

Ethical and Legal Considerations: Cloud forensic investigations raise significant ethical and legal considerations, including data privacy, jurisdictional issues and chain of custody requirements. Future research and practice must prioritize adherence to ethical standards and compliance with relevant laws and regulations to uphold the integrity and admissibility of digital evidence in legal proceedings.

In conclusion, the future of cloud forensic investigations hinges on embracing innovation, collaboration and standardization to address the challenges and complexities of cloud computing environments. By advancing capabilities, leveraging emerging technologies, and fostering interdisciplinary collaboration, researchers and practitioners can enhance the effectiveness, reliability and integrity of cloud forensic investigations, ultimately contributing to the resilience and security of digital ecosystems in the digital era.

REFERENCES

[1]. R. Ruan, K. Carthy, and T. Kechadi, "Cloud Forensics: An Overview," Proceedings of the International Conference on Availability, Reliability and Security, 2010.
[2]. A. Al Mutawa et al., "Taxonomy of Cloud Forensics," Journal.
[3]. T. Martini et al., "Cloud Forensic Challenges: A Survey and Future Research Directions," Future Generation Computer Systems, 2014.
[4]. T. Martini and R. Choo, "Cloud Storage Forensics: MEGA as a Case Study," Digital Investigation, 2015.
[5]. M. Hayes et al., "Ethical Challenges in Cloud Computing: Reflections on Recent Incidents," Proceedings of the International Conference on Cloud Computing Technology and Science, 2017.
[6]. K. Carthy et al., "CloudFence: Data Forensics for Cloud Storage Services," Digital Investigation, 2019.
[7]. S. Peer et al., "Forensic Analysis Framework for Virtualized Cloud Environments," Proceedings of the International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia, 2020.
[8]. Y. Khan et al., "Forensic Analysis of Cloud Storage Services: A Comparative Study," Digital Investigation, 2020.
[9]. J. Yamin et al., "Challenges and Limitations in Multi-Tenant Cloud Forensic Investigations," Journal of Cloud Computing: Advances, Systems and Applications, 2017.
[10]. R. Kanth et al., "Cloud Forensics: Challenges and Emerging Trends," Proceedings of the International Conference on Cloud Computing and Services Science, 2020.
[11]. T. Li et al., "Edge Computing Forensics: Challenges and Opportunities," Digital Investigation, 2019.
[12]. R. Ruan et al., "Encryption Technologies in Cloud Forensics: A Review," Proceedings of the International Conference on Information Systems Security and Privacy, 2019.
[13]. A. Slay et al., "A Conceptual Framework for Cloud Forensic Readiness," Journal of Digital Forensics, Security and Law, 2017.
[14]. T. Martini et al., "Jurisdictional Challenges in Cloud Forensics," Digital Investigation, 2016.
[15]. E. Kanth and S. Carthy, "Serverless Computing Forensics: A Review," Proceedings of the International Conference on Cyber Security and Protection of Digital Services, 2022.
[16]. N. Raghavan et al., "Regulatory Challenges in Cloud Forensics: A Comparative Analysis," Journal of Cloud Computing: Advances, Systems and Applications, 2018.
[17]. S. Martini et al., "Cloud Forensics: Current Trends and Future Directions," Proceedings of the International Conference on Digital Forensics and Cyber Crime, 2023.
[18]. T. Martini and K. Choo, "Guidelines for Ethical Conduct in Cloud Forensics Research," Digital Investigation, 2015.
[19]. J. Carthy et al., "Cloud Forensics Tool Landscape: A Comparative Analysis," Digital Investigation, 2021.
[20]. Park, Jun-Hak, Sang-Ho Na, Jun-Young Park, Eui-Nam Huh, Chul-Woo Lee, and Hyoung-Chun Kim, "A Study on Cloud Forensics and Challenges in SaaS Application Environment," in 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/Smart City/DSS), IEEE, 2016.
[21]. R. Montasari, "An Overview of Cloud Forensics Strategy: Capabilities, Challenges, and Opportunities," in Strategic Engineering for Cloud Computing and Big Data Analytics, Cham, Springer International Publishing, 2017, pp. 189-205.
[22]. S. Ali, S. Memon and F. Sahito, "Challenges and Solutions in Cloud Forensics," in Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing - ICCBDC'18, 2018.
[23]. A. Hosseinian, "Challenges of Cloud Forensics." Enterprise Security: Second International Workshop," in Revised Selected Papers, vol. 10131, Vancouver, BC: Springer, 2015.
[24]. N. Raza, "Challenges to network forensics in cloud computing," in 2015 Conference on Information Assurance and Cyber Security (CIACS), 2015.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13245

[25]. W. Mahmood, H. Jahankhani and A. Ozkaya, "Cloud Forensics Challenges Faced by Forensic Investigators," in Communications in Computer and Information Science, Cham, Springer International Publishing, 2015, pp. 74-82.

[26]. D. Freet, R. Agrawal, S. John and J. Walker, "Cloud forensics challenges from a service model standpoint," in Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital Eco Systems - MEDES '15, 2015.

[27]. Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S, "Cloud forensics: identifying the major issues and challenges," in International conference on

[28]. advanced information systems engineering, Springer, 2014.

[29]. Zargari, Shahrzad, and David Benford "Cloud forensics: Concepts, issues, and challenges," in 2012 Third International Conference on Emerging Intelligent Data and Web Technologies, Bucharest, 2012.

[30]. Shah, J. J., and Latesh G. Malik, "Cloud forensics: issues and challenges," in 2013 6th International Conference on Emerging Trends in Engineering and Technology, 2013.

[31]. A. Mishra, P. Matta, E. Pilli and R. Joshi, "Cloud Forensics: State-of-the-Art and Research Challenges," in 2012 International Symposium on Cloud and Services Computing, IEEE, 2012.

[32]. Pichan, Ameer, Mihai Lazarescu, and Sie Teng Soh, "Towards a practical cloud forensics logging framework," Journal of information security and applications, vol. 42, pp. 18--28, 2018.

[33]. X. Feng and Y. Zhao, "Digital Forensics Challenges to Big Data in the Cloud," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (Green Com) and IEEE Cyber, Physical and Social Computing (CPS Com) and IEEE Smart Data (Smart Data), IEEE, 2017.

[34]. L. Chen, L. Xu, X. Yuan and N. Shashidhar, "Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges," in 2015 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2015.

[35]. Poisel, Rainer, and Simon Tjoa, "Discussion on the challenges and opportunities of cloud forensics," in International Conference on Availability, Reliability, and Security, 2012

[36]. Pichan, Ameer, Mihai Lazarescu, and Sie Teng Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," Digital investigation, vol. 13, pp. 38--57, 2015.

[37]. S. Khan, "Cloud log forensics: Foundations, state of the art, and future directions," ACM Computing Surveys (CSUR), vol. 49, p. 1–42, 2016.

[38]. D. Gonzales, J. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," IEEE Transactions on Cloud Computing, vol. 5, pp. 523-536, 2015.

[39]. C. Federici, "Alma Nebula: A Computer Forensics Framework for the Cloud," Procedia Computer Science, vol. 19, pp. 139-146, 2013.

[40]. Povar, Digambar, and G. Geetha kumari, "A heuristic model for performing digital forensics in cloud computing environment," in International Symposium on Security in Computing and Communication, 2014

[41]. M. Ahsan, M. Ahsan, A. Wahab, M. Idris, S. Khan, E. Bachura and K.-K. R. Choo, "CLASS: Cloud Log Assuring Soundness and Secrecy Scheme for Cloud Forensics," IEEE Transactions on Sustainable Computing, pp. 1-1, 2016

[42]. Kumar Raju, B. K. S. P., and G. Geetha kumari, "Event correlation in cloud: a forensic perspective," Computing, vol. 98, no. 11, pp. 1203--1224, 2016.

[43]. S. Almulla, Y. Iraqi and A. Jones, "A Distributed Snapshot Framework for Digital Forensics Evidence Extraction and Event Reconstruction from Cloud Environment," in 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, vol. 1, IEEE, 2013.

[44]. S. S. Sampana, "Force (Forensic recovery of cloud evidence): A digital cloud forensics framework," in 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019

[45]. J. James and P. Gladyshev, "Challenges with automation in digital forensic investigations," 2013.

[46]. E. Hemdan, D. El-Din and Manjaiah, in CFIM: Toward Building New Cloud Forensics Investigation Model." Innovations in Electronics and Communication Engineering, Singapore, Springer, 2018, p. 545–554.

[47]. S. Zawoad and R. Hasan, "Chronos: Towards Securing System Time in the Cloud for Reliable Forensics Investigation," in 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), vol. 1, IEEE, 2016.

[48]. Zhang, Wei-Zhe, Hu-Cheng Xie, and Ching-Hsien Hsu., "Automatic Memory Control of Multiple Virtual Machines on a Consolidated Server," IEEE Transactions on Cloud Computing, vol. 5, pp. 2-14, 2015.

[49]. GetData, Virtual Forensics Computing, (https://www.virtualforensiccomputing.com/), [Accessed 30 June, 2015].

[50]. Wireshark, (https://www.wireshark.org/), [Acce ss ed 30 June, 2015].

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13245

[51]. Microsoft, Microsoft Expression Encoder4.,(http://www.microsoft.com/en-us/ download/details.aspx?id=18974), [Accessed 30 June, 2015].

[52]. FTK. Forensics tool kit (FTK) computer forensics software, (http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk), [Accessed 30 June 2015].

[53]. En Case, Guidance Software. (https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx), [Accessed 30 June, 2015].

[54]. Dykstra, J., & Sherman, A, "Design and implementation of FROST: digital forensic tools for the OpenStack cloud computing platform", Digital Investigation, Vol.10, Page: 87-95, 2013.

[55]. Xen Acess Library. (http://code.google.com/ p/xenaccess/), [Accessed 30 June, 2015]

