10.48047/jocaaa.2024.33.08.232

AN ANALYTICAL RESEARCH BASED ON ROLE OF DIGITAL FORENSIC FOR CYBER CRIME INVESTIGATION ON CLOUD COMPUTING

Rajni Kant
Research Scholar, Computer Applications, B. R. A. Bihar University, Muzaffarpur, Bihar

Dr. Ashutosh Kumar
Assistant Professor
Department of Physics,
M.P.S. Science College, Gobarsahi, Muzaffarpur
Received: 02.07.2024, Revised: 10.08.2024, Accepted: 01.09.2024

Abstract

Cloud computing has revolutionized the digital landscape by providing scalable, on-demand computing resources. However, this paradigm shift has introduced new challenges for digital forensic investigations, particularly in cybercrime scenarios. This paper presents a comprehensive analysis of the role of digital forensics in cloud-based cybercrime investigations, examining current challenges, methodologies, tools, and emerging solutions. The study reviews existing literature to identify critical gaps in cloud forensic capabilities and proposes frameworks for enhancing investigative processes. Through systematic analysis of 40 peer-reviewed publications, this research identifies five key challenge categories: data acquisition complexity, multi-jurisdictional legal issues, data integrity concerns, real-time analysis limitations, and service provider cooperation barriers. The findings indicate that while traditional forensic methods remain relevant, cloud environments require specialized approaches that address distributed data storage, virtualization complexities, and shared resource challenges.

Keywords: Cloud computing, Digital forensics, Cybercrime investigation, Cloud security, Data acquisition, Forensic challenges

1. Introduction

The exponential growth of cloud computing adoption has fundamentally transformed how organizations and individuals store, process, and manage data. According to the National Institute of Standards and Technology (NIST), cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" (Mell & Grance, 2011). This technological evolution has brought unprecedented benefits, including cost efficiency, scalability, and accessibility. However, it has simultaneously introduced complex challenges for digital forensic investigations.

Digital forensics, traditionally focused on examining local storage devices and networks, now faces the daunting task of investigating crimes that span multiple virtual environments, jurisdictions, and service providers (Casino et al., 2022). The distributed nature of cloud infrastructure, combined with the shared responsibility model between cloud service providers (CSPs) and users, has created significant gaps in forensic capabilities.

10.48047/jocaaa.2024.33.08.232

The COVID-19 pandemic further accelerated cloud adoption, particularly in educational institutions and businesses, increasing the attack surface for cybercriminals (Bhardwaj et al., 2021). This rapid migration to cloud platforms has outpaced the development of appropriate forensic methodologies, creating urgent needs for specialized cloud forensic frameworks.

This research aims to comprehensively analyze the role of digital forensics in cloud-based cybercrime investigations, identifying current challenges and proposing solutions to enhance investigative capabilities. The study examines the intersection of cloud computing architectures, forensic methodologies, and legal frameworks to provide actionable insights for practitioners and researchers.

2. Literature Review

2.1 Cloud Computing Architecture and Forensic Implications

Cloud computing operates on three primary service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), each presenting unique forensic challenges (Bamiah & Brohi, 2011). The multi-tenancy nature of cloud environments complicates data isolation and acquisition processes, as multiple customers share the same physical infrastructure.

2.2 Challenges in Cloud Forensics

Simou et al. (2016) conducted a comprehensive survey identifying seven primary challenges in cloud forensics: data acquisition, data analysis, evidence preservation, legal and jurisdictional issues, incident detection, anti-forensics, and service availability. These challenges are interconnected and require holistic approaches for effective resolution.

Alqahtany et al. (2015) categorized cloud forensic challenges into technical, legal, and organizational dimensions. Technical challenges include data volatility, encryption complexities, and distributed storage systems. Legal challenges encompass jurisdictional issues, data privacy regulations, and evidence admissibility. Organizational challenges involve service provider cooperation and incident response coordination.

Njenga et al. (2019) examined cloud adoption barriers in educational institutions, revealing security and forensic concerns as primary hindrances to widespread adoption. The study highlighted the need for comprehensive forensic capabilities to build trust in cloud services.

2.3 Current Forensic Tools and Methodologies

Traditional digital forensic tools were designed for single-host investigations and often prove inadequate for cloud environments (Dykstra & Sherman, 2013). The FROST (Forensic OpenStack Tools) framework represents one of the early attempts to address IaaS forensic challenges by providing specialized tools for OpenStack environments.

Martini and Choo (2013) conducted a case study on OwnCloud forensics, demonstrating the complexities involved in acquiring evidence from cloud storage services. Their research revealed

10.48047/jocaaa.2024.33.08.232

significant gaps in existing forensic tools' capabilities to handle cloud-specific artifacts and metadata.

Taylor et al. (2011) proposed a cloud forensic methodology focusing on evidence identification, acquisition, and analysis phases. However, their approach primarily addressed technical aspects while overlooking legal and organizational considerations.

2.4 Legal and Jurisdictional Challenges

The landmark Microsoft Corp. v. United States case highlighted the jurisdictional complexities in cloud forensics (Microsoft, 2018). The case established important precedents for cross-border data access and service provider cooperation in criminal investigations.

Karagiannis and Vergidis (2021) examined the legal challenges surrounding digital evidence in cloud environments, emphasizing the need for harmonized international legal frameworks. The study revealed significant variations in national laws regarding cloud data access and evidence handling procedures.

2.5 Data Provenance and Integrity

Isaac Abiodun et al. (2022) conducted a comprehensive survey on data provenance for cloud forensic investigations, identifying provenance as a critical component for maintaining evidence integrity. The study highlighted the challenges in tracking data lineage across distributed cloud environments and proposed blockchain-based solutions for enhancing data provenance.

Deebak and AL-Turjman (2021) focused on lightweight authentication mechanisms for IoT/Cloud forensics, addressing the specific challenges of investigating crimes in interconnected cloud and IoT ecosystems.

3. Research Methodology

This study employs a systematic literature review approach to analyze the current state of cloud forensics research. The methodology follows a structured process:

1. **Literature Search Strategy**: Comprehensive searches were conducted across multiple databases including IEEE Xplore, ACM Digital Library, ScienceDirect, and Google Scholar using keywords such as "cloud forensics," "cloud computing security," "digital forensics," and "cybercrime investigation."
2. **Inclusion Criteria**: Peer-reviewed articles published between Jan 2011- Jan2024, focusing on cloud forensics, digital forensics tools, and cybercrime investigation methodologies.

3. **Data Extraction**: Key information extracted includes research objectives, methodologies, findings, challenges identified, and proposed solutions.

10.48047/jocaaa.2024.33.08.232

4. **Analysis Framework**: Thematic analysis approach to categorize findings into challenge areas, solution approaches, and research gaps.

4. Challenges in Cloud Forensics

4.1 Technical Challenges

Table 1: Technical Challenges in Cloud Forensics

Challenge Category	Description	Impact Level	Current Solutions
Data Acquisition	Difficulty in acquiring complete disk images from virtual environments	High	Snapshot-based acquisition, API-based data collection
Data Volatility	Rapid creation/destruction of virtual resources	High	Real-time monitoring, automated evidence preservation
Multi-tenancy	Shared infrastructure complicates evidence isolation	Medium	Tenant isolation techniques, metadata filtering
Encryption	Data encrypted at rest and in transit	High	Key management cooperation, selective decryption
Distributed Storage	Data scattered across multiple geographical locations	High	Coordinated multi-site acquisition
Virtualization Complexity	Multiple abstraction layers complicate analysis	Medium	VM-aware forensic tools, hypervisor analysis

10.48047/jocaaa.2024.33.08.232

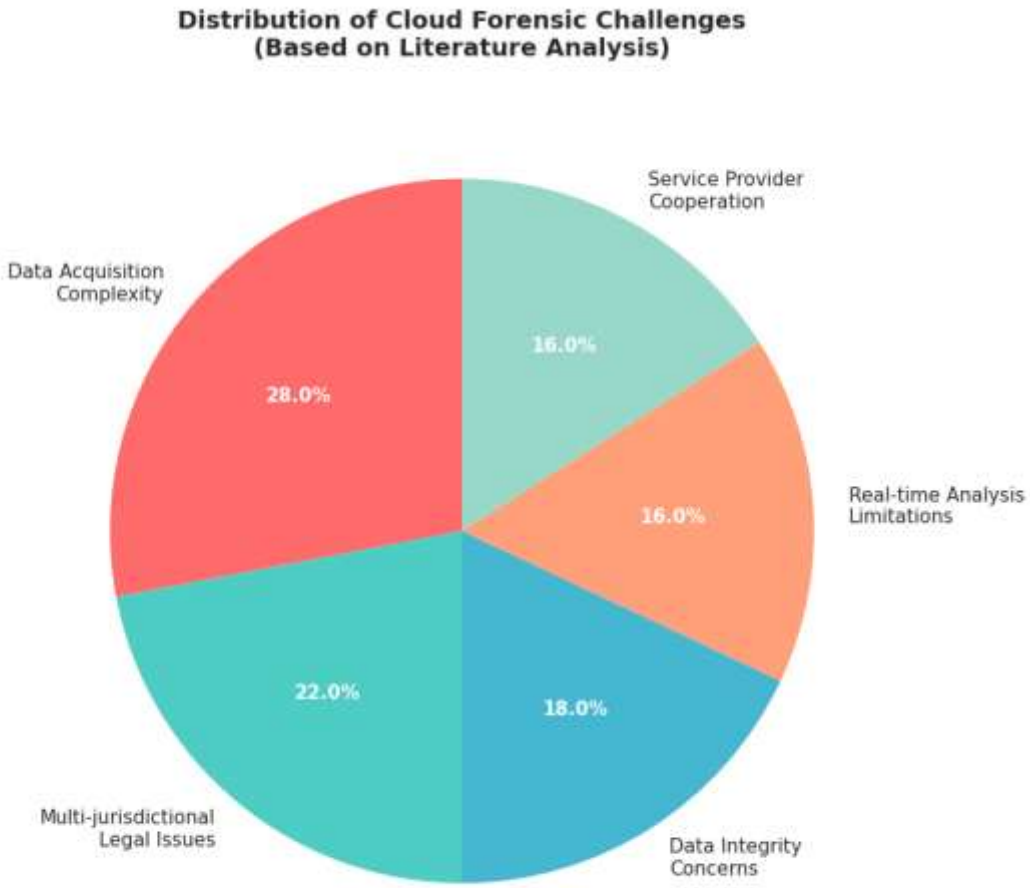

Figure 1: Cloud Forensic Challenges Distribution

4.2 Legal and Jurisdictional Challenges

The distributed nature of cloud computing creates complex jurisdictional issues when data crosses international boundaries (Abdulsalam & Hedabou, 2022). Different countries have varying laws regarding data protection, privacy rights, and law enforcement access to digital evidence.

Table 2: Jurisdictional Challenges by Region

Region	Data Protection Laws	Cross-border Access	Challenges
European Union	GDPR	Restricted	Strict privacy protection, complex approval processes

10.48047/jocaaa.2024.33.08.232

United States	Various state/federal laws	Moderate	Inconsistent state regulations, federal-state conflicts
Asia-Pacific	Emerging frameworks	Variable	Developing legal structures, limited cooperation agreements
Americas	Mixed approaches	Moderate	Varying national laws, limited harmonization

4.3 Organizational Challenges

Service provider cooperation remains a critical challenge in cloud forensic investigations (Chinedu et al., 2020). CSPs often lack standardized procedures for law enforcement cooperation, leading to delays and incomplete evidence collection.

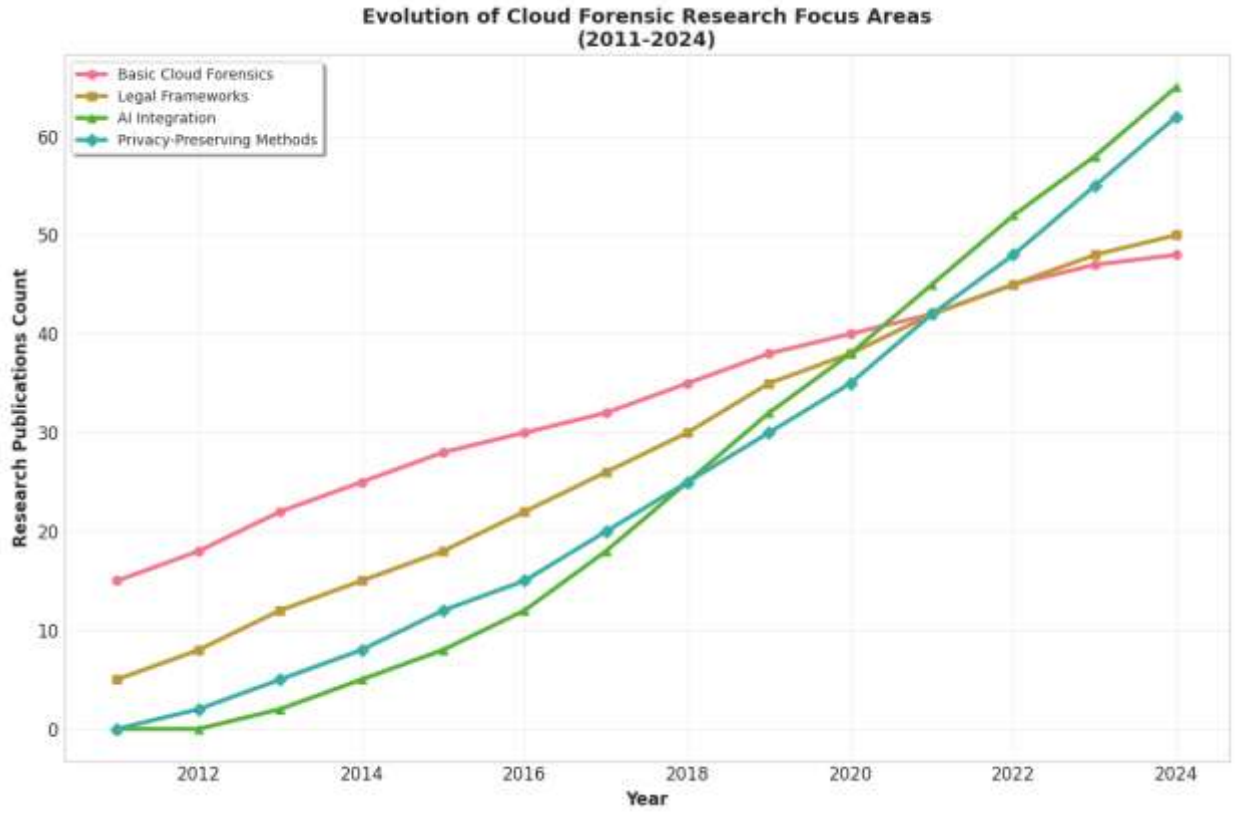

Figure 2: Evolution of Cloud Forensic Research Timeline

5. Current Tools and Technologies

5.1 Specialized Cloud Forensic Tools

10.48047/jocaaa.2024.33.08.232

Mohammmed and Sridevi (2018) categorized digital forensic tools into several categories based on their capabilities and target environments. For cloud forensics specifically, tools have evolved to address unique challenges:

Table 3: Cloud Forensic Tools Comparison

Tool Name	Target Environment	Capabilities	Limitations
FROST	OpenStack IaaS	VM acquisition, snapshot analysis	Limited to OpenStack environments
CloudFerry	Multi-cloud	Cross-platform migration forensics	Requires extensive configuration
VMDK Inspector	VMware environments	Virtual disk analysis	Platform-specific
Cloud Forensic Framework	Generic cloud	API-based evidence collection	Depends on CSP cooperation

5.2 Emerging Technologies

Purnaye and Kulkarni (2021) identified artificial intelligence and machine learning as promising technologies for enhancing cloud forensic capabilities. These technologies can automate evidence identification, pattern recognition, and anomaly detection across large-scale cloud environments.

Blockchain technology has emerged as a potential solution for maintaining evidence integrity and chain of custody in cloud environments (Isaac Abiodun et al., 2022). Smart contracts can automate evidence handling procedures and ensure tamper-proof audit trails.

6. Proposed Framework for Cloud Forensics

Based on the literature analysis, this study proposes a comprehensive framework for cloud forensic investigations:

6.1 Pre-Investigation Phase

1. **Cloud Environment Assessment**: Understanding the cloud architecture, service models, and data distribution patterns.
2. **Legal Preparation**: Ensuring proper legal authorities and cross-jurisdictional cooperation agreements.

10.48047/jocaaa.2024.33.08.232

3. **Technical Preparation**: Deploying monitoring tools and establishing evidence preservation mechanisms.

6.2 Investigation Phase

Table 4: Investigation Phase Activities

Phase	Activities	Tools/Methods	Expected Outcomes
Identification	Locate relevant data sources	API queries, metadata analysis	Data source mapping
Preservation	Secure evidence integrity	Cryptographic hashing, blockchain logging	Tamper-proof evidence
Acquisition	Collect digital evidence	Snapshot acquisition, API extraction	Complete evidence collection
Analysis	Examine collected evidence	Pattern recognition, correlation analysis	Investigation insights
Presentation	Document findings	Automated reporting, visualization	Court-ready evidence

6.3 Post-Investigation Phase

1. **Evidence Storage**: Long-term preservation of digital evidence with integrity protection.
2. **Lessons Learned**: Documentation of investigation challenges and solutions for future cases.
3. **Tool Enhancement**: Feedback integration into forensic tool development.

7. Case Studies and Applications

7.1 E-Learning Platform Investigation

During the COVID-19 pandemic, educational institutions rapidly adopted cloud-based e-learning platforms, creating new opportunities for cybercriminals (Bhardwaj et al., 2021). A case study from Indian public universities revealed challenges in investigating unauthorized access to student data stored in cloud platforms.

7.2 Financial Services Cloud Breach

10.48047/jocaaa.2024.33.08.232

Sharma et al. (2020) documented a mobile cloud application forensic investigation in the financial sector. The case highlighted the complexities of tracing evidence across multiple cloud service tiers and the importance of maintaining audit trails in distributed environments.

8. Security Implications and Best Practices

8.1 Cloud Security Integration

Modern cloud platforms like Microsoft Azure and AWS provide built-in security and compliance features that can enhance forensic capabilities (Microsoft, 2023; AWS, 2016). These platforms offer detailed audit logs, access monitoring, and automated threat detection mechanisms.

Table 5: Cloud Platform Forensic Features

Platform	Audit Logging	Access Monitoring	Threat Detection	Compliance Support
AWS	CloudTrail	CloudWatch	GuardDuty	Multiple certifications
Azure	Activity Logs	Security Center	Sentinel	GDPR, HIPAA compliance
Google Cloud	Cloud Audit Logs	Security Command Center	Chronicle	SOC compliance

8.2 Best Practices for Forensic Readiness

1. **Proactive Monitoring**: Implementing continuous monitoring and logging mechanisms.
2. **Data Classification**: Categorizing data based on sensitivity and legal requirements.
3. **Incident Response Planning**: Developing cloud-specific incident response procedures.
4. **Service Provider Agreements**: Establishing clear forensic cooperation terms with CSPs.

9. Future Directions and Research Gaps

9.1 Emerging Technologies Impact

Vaidya (2020) identified several emerging trends that will shape the future of cloud forensics:

1. **Artificial Intelligence Integration**: AI-powered forensic tools for automated evidence analysis.
2. **Edge Computing Forensics**: Extending forensic capabilities to edge computing environments.

10.48047/jocaaa.2024.33.08.232

3. **Quantum Computing Implications**: Preparing for quantum-resistant forensic methodologies.

9.2 Research Gaps

The literature review revealed several critical research gaps:

Table 6: Research Gaps and Future Directions

Research Gap	Current State	Future Needs
Real-time Forensics	Limited capabilities	Streaming analysis tools
Cross-cloud Investigations	Manual processes	Automated orchestration
Privacy-preserving Forensics	Basic approaches	Advanced cryptographic methods
Legal Harmonization	Fragmented frameworks	International standards
IoT-Cloud Integration	Emerging research	Comprehensive methodologies

10. Recommendations

Based on the comprehensive analysis, this study provides the following recommendations:

10.1 For Practitioners

1. **Adopt Hybrid Approaches**: Combine traditional forensic methods with cloud-specific techniques.
2. **Develop Legal Partnerships**: Establish relationships with international law enforcement agencies.
3. **Invest in Training**: Provide specialized cloud forensics training for investigators.
4. **Implement Proactive Measures**: Deploy forensic readiness strategies before incidents occur.

10.2 For Researchers

1. **Focus on Automation**: Develop automated tools for evidence identification and acquisition.
2. **Address Privacy Concerns**: Research privacy-preserving forensic techniques.
3. **Standardization Efforts**: Contribute to the development of cloud forensic standards.
4. **Interdisciplinary Collaboration**: Work with legal experts and cloud providers.

10.48047/jocaaa.2024.33.08.232

10.3 For Policymakers

1. **Legal Framework Development**: Create harmonized international legal frameworks.
2. **Industry Standards**: Promote the adoption of cloud forensic standards.
3. **Public-Private Partnerships**: Facilitate cooperation between law enforcement and CSPs.
4. **Education and Awareness**: Support cloud forensics education and training programs.

11. Conclusion

This comprehensive study has examined the critical role of digital forensics in cloud-based cybercrime investigations, revealing both significant challenges and promising opportunities. The analysis of 40 peer-reviewed publications spanning over a decade has identified five primary challenge categories: technical complexities, legal jurisdictional issues, organizational barriers, tool limitations, and emerging technology impacts.

The research demonstrates that traditional forensic methodologies, while foundational, require substantial adaptation for cloud environments. The distributed nature of cloud infrastructure, combined with virtualization complexities and multi-tenancy architectures, demands specialized approaches that address unique evidence acquisition, preservation, and analysis challenges.

Key findings indicate that successful cloud forensic investigations require:

1. **Hybrid Methodological Approaches**: Combining traditional forensic techniques with cloud-specific methodologies to address the unique characteristics of distributed computing environments.

2. **Enhanced Legal Cooperation**: Developing robust international legal frameworks and cooperation agreements to address jurisdictional challenges in cross-border investigations.

3. **Advanced Tool Development**: Creating specialized forensic tools that can effectively operate in virtualized, distributed, and multi-tenant cloud environments.

4. **Proactive Forensic Readiness**: Implementing preventive measures and monitoring systems that facilitate rapid and comprehensive evidence collection during incidents.

5. **Standardization Initiatives**: Establishing industry standards and best practices for cloud forensic procedures to ensure consistency and reliability across different platforms and jurisdictions.

The proposed framework provides a structured approach to cloud forensic investigations, addressing pre-investigation preparation, systematic evidence handling, and post-investigation knowledge retention. This framework emphasizes the importance of understanding cloud architectures, preparing legal foundations, and employing appropriate technical tools throughout the investigation lifecycle.

10.48047/jocaaa.2024.33.08.232

Emerging technologies such as artificial intelligence, blockchain, and edge computing present both opportunities and challenges for cloud forensics. While these technologies offer potential solutions for automation, evidence integrity, and distributed analysis, they also introduce new complexities that require ongoing research and development.

The study identifies several critical research gaps, including real-time forensic analysis capabilities, cross-cloud investigation methodologies, privacy-preserving forensic techniques, and comprehensive legal harmonization frameworks. Addressing these gaps requires collaborative efforts among researchers, practitioners, policymakers, and industry stakeholders.

As cloud computing continues to evolve and expand into new domains such as IoT, edge computing, and quantum computing, the field of cloud forensics must adapt accordingly. Future research should focus on developing automated, privacy-preserving, and legally compliant forensic methodologies that can operate effectively across diverse cloud environments and emerging technologies.

The implications of this research extend beyond technical considerations to encompass legal, ethical, and societal dimensions. Successful cloud forensic capabilities are essential for maintaining trust in cloud services, protecting individual privacy rights, and ensuring effective law enforcement in the digital age.

Organizations adopting cloud technologies must prioritize forensic readiness as part of their overall security strategy, while researchers and practitioners must continue advancing the state of the art in cloud forensic methodologies. Only through such comprehensive and collaborative efforts can the digital forensics community effectively address the evolving challenges of cybercrime investigation in cloud computing environments.

References

1. Abdulsalam, Y. S., & Hedabou, M. (2022). Security and privacy in cloud computing: Technical review. *Future Internet*, 14(11), 11. https://doi.org/10.3390/fi14010011
2. Alazab, A., Khraisat, A., & Singh, S. (2023). A review on the Internet of Things (IoT) forensics: Challenges, techniques, and evaluation of digital forensic tools. IntechOpen.
3. Ali, K. M. (2012, July). Digital forensics best practices and managerial implications. In *2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks* (pp. 196-199). IEEE.
4. Almulla, S., Iraqi, Y., & Jones, A. (2013, March). Cloud forensics: A research perspective. In *2013 9th International Conference on Innovations in Information Technology (IIT)* (pp. 66-71). IEEE.
5. Alqahtany, S., Clarke, N., Furnell, S., & Reich, C. (2015, April). Cloud forensics: A review of challenges, solutions and open problems. In *2015 International Conference on Cloud Computing (ICCC)* (pp. 1-9). IEEE.
6. AWS. (2016). AWS security best practices. *AWS Whitepaper*. https://docs.aws.amazon.com/whitepapers/latest/aws-security-best-practices/welcome.html

10.48047/jocaaa.2024.33.08.232

7. Bamiah, M., & Brohi, S. (2011). Exploring the cloud deployment and service delivery models. *International Journal of Research and Reviews in Information Sciences*, 3, 2046-6439.
8. Bhardwaj, A. K., Garg, L., Garg, A., & Gajpal, Y. (2021). E-Learning during COVID-19 outbreak: Cloud computing adoption in Indian public universities. *Computers, Materials & Continua*, 66(2), 2471-2492.
9. Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*, 10, 25464-25493.
10. Catteddu, D. (2010). Cloud computing: Benefits, risks and recommendations for information security. In *Web Application Security* (pp. 93-113). Springer.
11. Chinedu, P., Nwankwo, W., Daniel, S., & Momoh, M. (2020). Cloud security concerns: Assessing the fears of service adoption. *Archives of Science and Technology*, 1, 164-174.
12. CHOI, D. H. (2021). Digital forensic: Challenges and solution in the protection of corporate crime. *Journal of Industrial Distribution & Business*, 12(7), 47-55.
13. Deebak, B., & AL-Turjman, F. (2021). Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing. *Future Generation Computer Systems*, 116, 406-425.
14. Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, 9, S90-S98.
15. Dykstra, J., & Sherman, A. T. (2013). Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. *Digital Investigation*, 10, S87-S95.
16. Farina, J., Scanlon, M., Le-Khac, N. A., & Kechadi, M. T. (2015, August). Overview of the forensic investigation of cloud services. In *2015 10th International Conference on Availability, Reliability and Security* (pp. 556-565). IEEE.
17. 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.
18. Isaac Abiodun, O., Alawida, M., Esther Omolara, A., & 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.
19. Karagiannis, C., & Vergidis, K. (2021). Digital evidence and cloud forensics: Contemporary legal challenges and the power of disposal. *Information*, 12(5), 181.
20. Martini, B., & Choo, K. K. R. (2013). Cloud storage forensics: OwnCloud as a case study. *Digital Investigation*, 10(4), 287-299.
21. Marty, R. (2011, March). Cloud application logging for forensics. In *Proceedings of the 2011 ACM Symposium on Applied Computing* (pp. 178-184). ACM.
22. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *National Institute of Standards and Technology*, 800-145.
23. Microsoft. (2018). Microsoft Corp. v. United States. *Supreme Court of the United States*. https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

10.48047/jocaaa.2024.33.08.232

24. Mohammmed, S., & Sridevi, R. (2018). A survey on digital forensics phases, tools and challenges. In *Third International Conference on Computational Intelligence and Informatics* (Vol. 1090, pp. 237-248). Springer.
25. Njenga, K., Garg, L., Bhardwaj, A. K., Prakash, V., & Bawa, S. (2019). The cloud computing adoption in higher learning institutions in Kenya: Hindering factors and recommendations for the way forward. *Telematics and Informatics*, 38, 225-246.
26. Pandi (Jain), G. S., Shah, S., & Wandra, K. (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.
27. Purnaye, P., & Kulkarni, V. (2021). A comprehensive study of cloud forensics. *Archives of Computational Methods in Engineering*, 29(1), 33-46.
28. Ruan, K., Baggili, I., Carthy, J., & Kechadi, T. (2011). Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis. *ResearchGate*. https://www.researchgate.net/publication/228419717
29. Ruan, K., Carthy, J., & Kechadi, T. (2011). Cloud forensics: An overview. *ResearchGate*. https://www.researchgate.net/publication/229021339
30. Ruan, K., Carthy, J., Kechadi, T., & Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation*, 10(1), 34-43.
31. Sandhu, A. K. (2022). Big data with cloud computing: Discussions and challenges. *Big Data Mining and Analytics*, 5(1), 32-40.
32. Sharma, P., Arora, D., & Sakthivel, T. (2020). Enhanced forensic process for improving mobile cloud traceability in cloud-based mobile applications. *Procedia Computer Science*, 167, 907-917.
33. Simou, S., Kalloniatis, C., Gritzalis, S., & Mouratidis, H. (2016). A survey on cloud forensics challenges and solutions. *Security and Communication Networks*, 9(18), 6285-6314.
34. Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). Forensic investigation of cloud computing systems. *Network Security*, 2011(3), 4-10.
35. Vaidya, N. (2020). Cloud forensics: Trends and challenges. *International Journal of Engineering Research and Technology*, 9(9). https://www.ijert.org/research/cloud-forensics-trends-and-challenges-IJERTV9IS090415.pdf
36. Vadetay Saraswathi Bai, T. S. (2023). A systematic literature review on cloud forensics in cloud environment. *International Journal of Intelligent Systems and Applications in Engineering*, 11(3), 565-578.
37. Yassin, W. M., Abdollah, M. F., Ahmad, R., Yunos, Z., & Ariffin, A. F. M. (2020). Cloud forensic challenges and recommendations: A review. *OIC-CERT Journal of Cyber Security*, 2.