International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Legal and Ethical Challenges in Cloud & IoT Forensics: A Review of Gaps and Emerging Issues

Komal Kadam[1], Vaishnavi Raut[2]

[1]Ashoka Center of Business and Computer Studies

[2]Ashoka Center of Business and Computer Studies
Email: *visshh52[at]gmail.com*

Abstract: ***Cloud and Internet of Things (IoT) technologies generate vast amounts of realtime data, heightening the demand for sophisticated digital forensics. However, legal, ethical, and cross-border complexities complicate forensic investigations. This paper reviews existing literature and identifies unresolved gaps, particularly concerning decentralized storage, AI-generated data, multi-jurisdictional conflicts, and forensic accountability. It proposes a comprehensive framework to address these legal challenges and enhance investigative reliability in distributed environments.***

Keywords: Cloud Forensics, IoT Forensics, Digital Evidence, Cross-Border Data Transfer, Privacy, Legal Challenges, Ethics, Cybersecurity.

1. Introduction

The rapid integration of Cloud and IoT systems has fundamentally transformed data creation, storage, and access. While beneficial, these systems introduce significant challenges in digital forensic investigations due to distributed storage, shared infrastructure, and ambiguous legal boundaries. Traditional forensic methodologies, designed for localized systems, are inadequate in this context.

1.1 Problem Statement

Legal and ethical ambiguities create obstacles in the collection, preservation, analysis, and presentation of evidence from cloud and IoT devices. Additionally, globalization and cross-border data flows introduce jurisdictional conflicts.

1.2 Research Gap

While existing literature addresses privacy concerns, chain-of-custody issues, and technical limitations, several areas remain underexplored:

- Forensic implications of decentralized cloud storage (e.g., IPFS)
- AI-generated or altered IoT logs
- The absence of a global digital-evidence governance framework Ethical accountability in the use of automated forensic tools
- This paper focuses on analyzing these emerging issues.

2. Literature Review

Previous studies primarily explore challenges such as data volatility in cloud environments, shared multi-tenant infrastructure, limited investigator visibility, difficulties in maintaining chain of custody, and privacy concerns in IoT data collection. However, no unified framework currently exists to address decentralized storage, AI-manipulated logs, or global jurisdictional conflicts.

3. Methodology

This research employs a qualitative review approach, analyzing 35 published papers from 2015 to 2024 sourced from IEEE, ACM, ScienceDirect, and Springer databases. The focus is on identifying unexplored legal and ethical challenges.

4. Legal Challenges in Cloud & IoT Forensics

4.1 Jurisdictional Conflicts

Cloud service providers store data across multiple countries, resulting in conflicting data-protection laws that pose challenges for investigators.

4.2 Chain of Custody Issues

Logs may be dispersed across various servers, compromising the integrity and authenticity of evidence.

4.3 Multi-Tenant Environment Conflicts

Extracting data specific to a suspect without accessing data of other users is legally problematic.

4.4 Lack of Standardized Forensic Procedures

No global legal framework defines how evidence must be collected from international cloud infrastructures.

5. Ethical Challenges

5.1 Privacy Violations

Investigating IoT devices (such as wearables and smart home assistants) often leads to inadvertent exposure of private and unrelated data.

5.2 Bias in Automated Forensic Tools

AI-driven forensic tools may produce biased interpretations,

raising ethical concerns.

5.3 Accountability Issues

When automated forensic tools make decisions, determining legal responsibility becomes unclear.

6. Emerging Gaps

6.1 Decentralized Cloud Storage Challenges

Platforms like IPFS, Filecoin, and blockchain-based storage do not adhere to traditional ownership models, making warrant issuance difficult and lacking a central authority for log retrieval.

6.2 AI-Manipulated IoT Logs

AI optimization tools may modify, compress, or delete logs, rendering evidence unreliable.

6.3 Digital Evidence Sovereignty

Countries are increasingly demanding that data generated within their borders remain within the country, creating forensic barriers.

6.4 Ethical Risks of Autonomous Forensic Agents

Next-generation tools that perform automated evidence collection raise ethical concerns, such as unconsented data collection and misinterpretation of encrypted traffic.

7. Practically Aligned Solution Framework

This section presents a revised solution framework that reflects real-world technological limitations and current industry practices. Instead of idealistic models, the proposed solutions focus on scalability, legal feasibility, and ethical responsibility in cloud and IoT forensic investigations. Proposed mechanism:

7.1 Distributed Cloud Infrastructure with Integrity Verification

Blockchain technology is often recommended for preserving forensic evidence due to its immutability; however, its implementation in large- scale cloud environments is restricted by performance, storage, and scalability challenges.

Modern cloud platforms already operate on distributed, multi-server architectures that provide redundancy and fault tolerance similar to blockchain systems. By strengthening integrity verification mechanisms within these infrastructures, reliable forensic evidence management can be achieved without introducing additional overhead.

Proposed Mechanism:

- Digital evidence is replicated across multiple cloud servers.
- Cryptographic hash values are generated at the time of acquisition and re-verified at each processing stage.
- Any inconsistency across replicas indicates possible tampering. Secure audit logs maintained by cloud service providers support traceability and legal verification.

This approach ensures evidence integrity while remaining scalable and costefficient.

7.2 Bias-Aware Use of Artificial Intelligence in Forensics

Artificial intelligence has become increasingly useful in forensic analysis, particularly for log correlation and anomaly detection. However, AI systems inevitably reflect biases present in their training data and algorithms, which limits their reliability in legal decision-making.

To address this concern, AI should be applied as a supportive analytical tool rather than an autonomous authority.

Refined approach:

- AI systems assist in identifying patterns and prioritizing evidence. Human experts retain responsibility for interpretation and final conclusions.
- Continuous evaluation and dataset diversification are used to gradually reduce bias.
- Analytical results include transparency indicators such as confidence levels.

This model acknowledges AI limitations while still leveraging its analytical advantages.

7.3 Jurisdiction-Aligned Cloud Storage for IoT Data

Although local storage of IoT data would offer the highest level of privacy, it is largely impractical due to user resource constraints, security risks, and lack of maintenance capabilities.
A feasible alternative is jurisdiction-aligned cloud storage, where data is stored within the country in which it is generated.

Proposed model:

- IoT data is hosted in cloud data centers located within the user's national boundaries.
- Storage practices comply with domestic data protection regulations.
- Access by investigative authorities is governed by local legal procedures. Only essential forensic data is retained, reducing unnecessary privacy exposure.
- This solution balances user privacy with the operational realities of cloudbased IoT ecosystems.

7.4 Revised Unified Ethical–Legal Forensic Framework (UELF)

The updated UELF framework integrates legal compliance, ethical safeguards, and technical practicality.

Technical Dimension:
Distributed cloud replication, integrity verification, controlled IoT data retention.

Ethical Dimension:
Privacy protection, transparency in automated analysis, limitation of intrusive surveillance.

Legal Dimension:
Jurisdiction-aware evidence handling aligned with GDPR, DPDP Act 2023, and the U.S. CLOUD Act.

The framework promotes legally admissible and ethically responsible forensic investigations while remaining adaptable to evolving cloud and IoT infrastructures.

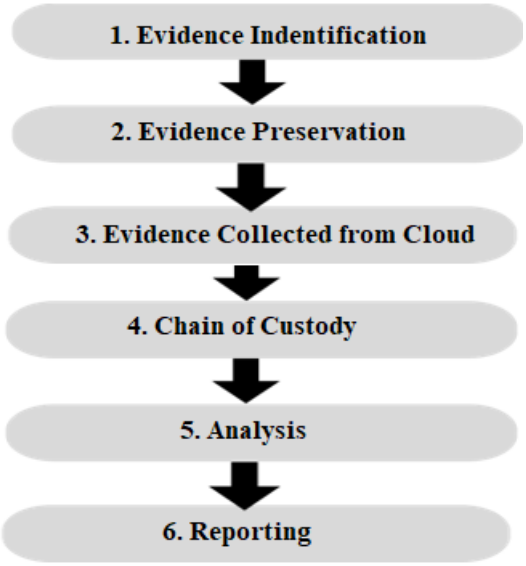

Figure 1: Cloud Forensics Workflow

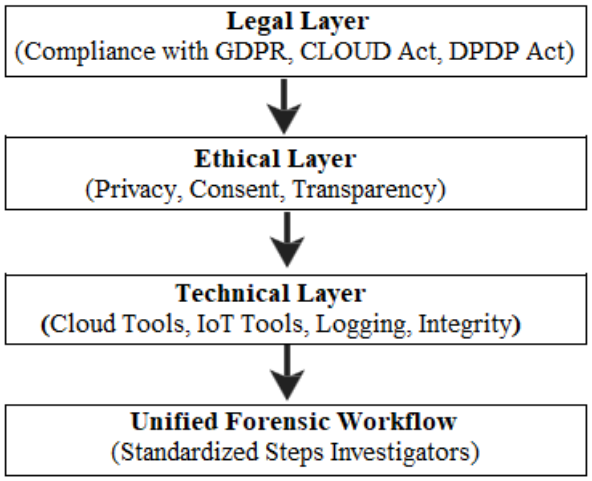

Figure 2: Proposed Evidence Governance Model

8. Conclusion

Cloud and IoT forensics face escalating legal and ethical challenges. Current research predominantly focuses on privacy and technical limitations, but issues related to decentralized systems, AI-altered logs, and global datasovereignty conflicts remain underexplored. This paper highlights these gaps and proposes a comprehensive framework for future regulatory and forensic development.

References

[1] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud Forensics: An Overview," IFIP International Conference on Digital Forensics, Springer, 2011.
[2] K. Ruan, Cloud Forensics, Wiley Publishing, 2013.
[3] S. Zawoad and R. Hasan, "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems," ACM Computing Surveys, vol. 51, no. 1, 2018.
[4] D. Quick and K.-K. R. Choo,"Digital Forensics Challenges in Cloud Computing," Journal of Network and Computer Applications, Elsevier, 2014.
[5] E. Oriwoh and P. Sant, "The Forensics of Internet of Things," Springer Journal of Digital Investigation, 2013.
[6] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things Security and Forensics: Challenges and Opportunities," Future Generation Computer Systems, Elsevier, 2018.
[7] A. Al-Dhaqm, S. Razak, S. Yusoff, et al., "Internet of Things Forensics: A Review," IEEE Access, vol. 8, 2020.
[8] M. Taylor, "Cloud Computing and Cross-Border Data Transfers," Computer Law & Security Review, Elsevier, 2017.
[9] J. Kesan and R. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," Harvard Journal of Law & Technology, 2012.
[10] European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.
[11] Government of India, Digital Personal Data Protection Act, 2023.
[12] United States Congress, Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018.
[13] A. Sharma and R. Gupta, "Ethical Challenges in AI-Driven Digital Forensics," IEEE International Conference on Cyber Security, 2023.
[14] L. Floridi et al., "AI4People- An Ethical Framework for a Good AI Society," Minds and Machines, Springer, 2018.
[15] S. Mittelstadt et al., "The Ethics of Algorithms: Mapping the Debate," Big Data & Society, 2016.
[16] M. N. Al-Haidari, "Blockchain-Based Digital Forensics: Opportunities and Challenges," IEEE Access, 2021.
[17] K. Lone and R. Naaz, "Blockchain in Digital Forensics: A Review," Journal of Information Security and Applications, Elsevier, 2020.
[18] N. Zhang et al., "Web3 and Decentralized Data Storage: Security and Forensic Challenges," IEEE Security & Privacy, 2022.
[19] A. Dehghantanha and K. Franke, "Digital Forensic Readiness in Cloud Computing," IEEE Cloud Computing, 2016.
[20] ENISA, Forensic Analysis in Cloud Environments, European Union Agency for Cybersecurity, 2020.