International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 3 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

A Review on Digital Forensics

P KUTTI[1] LECTURER IN IT DEPARTMENT OF INFORMATION TECHNOLOGY, RAJIV GANDHI UNIVERSITY OF KNOWLEDGE TECHNOLOGIES - SRIKAKULAM RESEARCH SCHOLAR-PART TIME(SRI VENKATESWARA UNIVERSITY) DEPARTMENT OF COMPUTER SCIENCE.SVU COLLEGE OF CM&CS TIRUPATHI Mail id: kuttypalyam@gmail.com
Dr.G.V.RAMESH BABU[2] ASSOCIATE PROFESSOR DEPARTMENT OF COMPUTER SCIENCE SVU COLLEGE OF CM&CS TIRUPATHI. Mail id: rameshbabugv@svumail.edu.in

Abstract: Digital forensics has become a critical discipline in modern cybersecurity and criminal investigations due to the rapid growth of digital technologies, cloud services, Internet of Things (IoT) devices, artificial intelligence, and decentralized computing environments. The increasing volume, velocity, and diversity of digital evidence have significantly transformed forensic investigation practices. Traditional forensic approaches based on static disk imaging are no longer sufficient for handling volatile, distributed, and encrypted data sources. This review examines the evolution of digital forensics from conventional computer investigations to contemporary cloud, IoT, cryptocurrency, and AI-driven environments. The paper explores emerging challenges including evidence acquisition, chain of custody preservation, anti-forensic techniques, privacy concerns, and the admissibility of AI-generated evidence. Furthermore, recent advances in machine learning-assisted investigations, deepfake detection, and automated forensic triage are analyzed. The review synthesizes current literature, identifies research gaps, and highlights future directions for developing scalable, intelligent, and legally defensible forensic frameworks.

Keywords: Digital Forensics, Chain of Custody, Cloud Forensics, Artificial Intelligence, Deepfake Detection, Anti-Forensics, Cryptocurrency Forensics, Triage Automation.

I. Introduction

Digital forensics has emerged as one of the most important disciplines within cybersecurity and criminal investigations. As societies become increasingly dependent on digital technologies, the amount of information generated by computers, mobile devices, cloud infrastructures, social media platforms, and Internet-connected systems continues to grow at an unprecedented rate. Every digital interaction leaves traces that can potentially serve as evidence during criminal investigations, civil litigation, corporate audits, and national security operations. Consequently, digital forensics has evolved from a niche technical field into a critical component of modern law enforcement and incident response frameworks **[1]**.

Historically, digital forensic investigations focused primarily on standalone computers and storage media. Investigators acquired forensic images of hard disks and examined them using specialized tools to identify deleted files, internet browsing history, emails, and system logs. However, technological developments over the past decade have dramatically altered the nature of digital evidence. Cloud computing, virtualization, blockchain technologies, artificial intelligence systems, and Internet of Things (IoT) devices have introduced new sources of evidence while simultaneously increasing investigative complexity. Modern

evidence may exist across multiple geographical regions, cloud providers, virtual environments, and encrypted communication channels **[2]**.

Despite significant advances in forensic technologies, investigators continue to face challenges associated with data volume, encryption, privacy regulations, anti-forensic techniques, and cross-jurisdictional legal constraints. These challenges necessitate the development of innovative forensic frameworks capable of operating effectively within complex digital ecosystems**[5]**.

1.1 Context and Modern Investigative Realities

The contemporary digital environment is characterized by interconnected systems, distributed computing infrastructures, and continuous data generation. Organizations increasingly utilize cloud platforms, remote work environments, edge computing architectures, and mobile applications to support operational activities. While these technologies provide substantial benefits, they also generate vast quantities of digital artifacts that investigators must analyze during forensic examinations **[6]**.

Modern investigations frequently involve multiple data sources including system logs, cloud storage repositories, network traffic records, social media interactions, cryptocurrency transactions, and IoT-generated telemetry. Unlike traditional computing environments where evidence resided on a single physical device, contemporary evidence may be fragmented across numerous platforms and jurisdictions. Investigators must therefore employ advanced collection and correlation techniques to reconstruct events accurately **[7].**

1.2 The Data Volume and Volatility Crisis

One of the most significant challenges confronting digital forensics is the exponential growth of digital data. Modern organizations generate terabytes of information daily through operational systems, cloud applications, security tools, and user activities. Processing such large datasets using conventional forensic techniques is increasingly impractical **[9]**.

Another challenge involves evidence volatility. Data stored in volatile memory may disappear when systems are powered down, while cloud-based resources may be automatically terminated without preserving forensic artifacts. Investigators must therefore collect evidence rapidly before critical information is lost.

1.3 Scope and Methodology of this Review

This review examines contemporary developments in digital forensics by synthesizing findings from recent scholarly publications, industry reports, and forensic frameworks. The analysis focuses on cloud forensics, IoT investigations, artificial intelligence applications, cryptocurrency tracing, anti-forensic methodologies, and legal challenges affecting digital evidence.

The review adopts a thematic approach by organizing literature according to major technological and investigative domains. Through critical synthesis of existing studies, this review aims to provide a comprehensive understanding of the current state of digital forensics and its future trajectory [13]**.**

II. Evolution of the Forensic Paradigm

The field of digital forensics has undergone substantial transformation since its emergence in the late twentieth century. Early investigations concentrated on

recovering evidence from personal computers and magnetic storage devices. Investigators relied heavily on disk imaging technologies and manual examination techniques to identify relevant artifacts. Although these methods remain important, they are increasingly insufficient for addressing modern investigative requirements.

This transformation has led to the development of specialized forensic disciplines including cloud forensics, network forensics, memory forensics, blockchain forensics, and IoT forensics. Each discipline addresses unique technical challenges while contributing to a broader understanding of digital investigations. Modern forensic methodologies increasingly emphasize automation, scalability, and real-time analysis to accommodate growing evidence volumes and operational complexity.

The transition from static to dynamic forensic environments has significantly transformed modern investigations.

2.1 Traditional Post-Mortem Forensics vs. Real-Time Triage

Traditional forensic investigations relied on post-mortem analysis, where investigators examined systems after incidents occurred. Evidence acquisition typically involved creating forensic copies of storage devices followed by detailed offline examination. This methodology ensured evidence preservation and reproducibility while minimizing contamination risks.

However, contemporary environments increasingly require real-time investigative capabilities. Cyberattacks may occur rapidly, and volatile evidence can disappear within minutes. Real-time triage methodologies enable investigators to identify critical artifacts quickly and prioritize evidence collection activities. Automated triage tools significantly reduce investigation time while improving operational efficiency.

2.2 Standardized Frameworks

Forensic investigations must maintain evidence integrity throughout the investigative lifecycle. Standardized frameworks developed by NIST, ISO, and law enforcement agencies provide structured procedures for evidence collection, preservation, analysis, and reporting. These frameworks help ensure consistency, reliability, and legal admissibility.

Chain of custody documentation remains particularly important because it demonstrates that evidence has not been altered or tampered with during an investigation. Courts increasingly require detailed documentation regarding evidence acquisition methods, analytical procedures, and validation processes. Consequently, forensic practitioners must balance technical effectiveness with legal defensibility when conducting investigations.

III Architectural Frontiers

The rapid evolution of computing architectures has fundamentally transformed the landscape of digital forensic investigations. Traditional forensic methodologies were developed primarily for standalone computing systems where investigators possessed direct physical access to storage media and system resources. However, modern digital infrastructures increasingly rely on cloud computing, edge

computing, Internet of Things (IoT) ecosystems, and decentralized blockchain networks. These environments offer significant operational advantages but simultaneously introduce substantial challenges for forensic practitioners.

Unlike traditional systems, contemporary digital environments distribute data across multiple physical locations, service providers, and virtualized infrastructures. Digital evidence may reside within cloud storage platforms, virtual machines, distributed ledgers, edge devices, and interconnected sensor networks. Furthermore, many of these environments generate highly volatile data that may disappear rapidly due to automatic system processes, resource reallocation, or user actions. Consequently, investigators must develop specialized techniques capable of identifying, collecting, preserving, and analyzing evidence within these complex architectures.

Recent research has emphasized the need for adaptive forensic frameworks that accommodate emerging technological paradigms while maintaining evidence integrity and legal admissibility. The following subsections examine major developments in cloud forensics, IoT forensics, and cryptocurrency investigations that represent the forefront of contemporary digital forensic research.

3.1 Virtualized Artifact Acquisition in Multi-Tenant Cloud Environments

One of the primary difficulties in cloud forensics arises from the absence of direct physical access to underlying hardware resources. Traditional forensic investigations rely on acquiring complete forensic images of storage devices. In cloud environments, investigators often depend on service providers to obtain relevant artifacts such as virtual machine snapshots, access logs, audit records, and storage images. This dependency may complicate evidence collection procedures and raise concerns regarding trust, transparency, and chain of custody preservation.

Another challenge stems from the multi-tenant nature of cloud infrastructures. Multiple customers frequently share the same physical hardware resources while remaining logically isolated through virtualization technologies. Investigators must ensure that evidence collection activities do not inadvertently compromise the privacy or security of other tenants. This requirement introduces legal and technical constraints that may limit forensic access to relevant information.

Virtualization technologies further complicate forensic investigations because virtual machines are highly dynamic. Cloud instances may be automatically created, migrated, resized, or terminated based on operational demands. Consequently, critical evidence may exist only temporarily before being overwritten or deleted. Researchers have therefore proposed proactive evidence preservation strategies including continuous logging, snapshot automation, and forensic readiness frameworks.

3.2 New Era Forensic Challenges:

Despite their evidentiary value, IoT devices present numerous forensic challenges. Many devices possess limited computational resources, restricted storage capacities, and proprietary operating systems. These characteristics often prevent the

implementation of conventional forensic acquisition techniques. Furthermore, manufacturers frequently employ proprietary communication protocols and data formats, making artifact interpretation difficult.

Another significant challenge involves the heterogeneity of IoT ecosystems. Investigators may encounter hundreds of device types originating from different vendors, each utilizing unique hardware architectures, software configurations, and communication mechanisms. Developing universal forensic methodologies capable of supporting such diversity remains a substantial research challenge.

The distributed nature of IoT environments further complicates evidence acquisition. Relevant artifacts may reside simultaneously on local devices, edge computing nodes, cloud servers, and mobile applications. Effective investigations therefore require coordinated collection strategies capable of correlating evidence across multiple platforms.

3.3 Digital Forensics and crypto

Contrary to common misconceptions, most blockchain networks are not entirely anonymous. Instead, they operate using pseudonymous addresses that record transactions on publicly accessible distributed ledgers. This transparency provides investigators with opportunities to analyze transaction histories and identify suspicious financial activities. Blockchain forensic techniques leverage transaction graph analysis, clustering algorithms, pattern recognition methods, and intelligence correlation strategies to attribute activities to specific entities.

However, cryptocurrency investigations face numerous challenges. Criminal actors frequently employ obfuscation mechanisms including mixing services, tumblers, privacy-focused cryptocurrencies, decentralized exchanges, and cross-chain transaction protocols. These techniques complicate transaction tracing efforts by obscuring relationships between sending and receiving addresses.

Privacy-enhancing cryptocurrencies such as Monero and Zcash present additional difficulties because they utilize advanced cryptographic mechanisms designed to conceal transaction details. Traditional blockchain analysis methods often prove ineffective against these technologies, requiring investigators to develop alternative intelligence-gathering approaches.

IV. AI based Algorithmic Investigations

Artificial intelligence has emerged as an important tool for improving the efficiency and scalability of digital forensic investigations.

4.1 Machine Learning for Automated Log Triaging and Anomaly Detection

One of the most promising applications of artificial intelligence in digital forensics involves automated log analysis and anomaly detection. Modern information systems generate enormous volumes of logs documenting user activities, network communications, application events, security alerts, and system operations. Manual examination of these datasets is time-consuming and often impractical, particularly during large-scale investigations.

Recent research demonstrates that AI-driven triage systems can substantially reduce investigation times while maintaining high levels of accuracy. Automated prioritization

mechanisms enable investigators to focus on the most relevant evidence first, thereby accelerating incident response activities. Nevertheless, machine learning systems remain dependent on training data quality and may produce inaccurate results when encountering unfamiliar scenarios. Consequently, human oversight remains essential throughout the investigative process.

4.2 Visual Forensics in the AI Era

The emergence of generative artificial intelligence has created new challenges for digital forensic investigations. Advanced deep learning models are now capable of generating highly realistic images, videos, audio recordings, and textual content that closely resemble authentic media. Commonly referred to as deepfakes, these synthetic artifacts have significant implications for cybersecurity, law enforcement, journalism, and judicial systems.

Modern deepfake detection systems increasingly employ machine learning algorithms trained to identify subtle statistical patterns within synthetic content. These systems analyze facial landmarks, frequency-domain characteristics, compression artifacts, and temporal inconsistencies across video frames. Some approaches also examine metadata, device signatures, and provenance information to verify media authenticity.

4.3 AI Evidence

Although artificial intelligence offers substantial benefits for digital forensic investigations, its adoption raises important concerns regarding transparency, accountability, and legal admissibility. Many advanced machine learning models operate as "black boxes," producing predictions or classifications without providing clear explanations for their decisions. This lack of interpretability presents significant challenges in forensic and legal contexts where evidence must be understandable, reproducible, and defensible.

Judicial systems generally require investigators to explain how evidence was obtained, analyzed, and interpreted. When AI systems generate investigative findings, courts may question whether those findings can be independently verified. If investigators cannot adequately explain the reasoning behind an AI-generated conclusion, the evidentiary value of that conclusion may be challenged.

To address these challenges, researchers are increasingly focusing on Explainable Artificial Intelligence (XAI). Explainable AI techniques provide human-understandable justifications for algorithmic decisions by identifying influential features, decision pathways, and confidence levels. These capabilities improve transparency and facilitate independent validation of forensic findings.

V. Obstructive Activities in Digital Forensics

As digital forensic techniques continue to advance, cybercriminals and malicious actors have simultaneously developed sophisticated methods designed to conceal, manipulate, destroy, or obstruct digital evidence. These techniques, collectively known as counter-forensics or anti-forensics, pose significant challenges to investigators by reducing the availability, reliability, and integrity of digital artifacts. The primary objective of counter-forensics is to prevent forensic

analysts from recovering evidence, reconstructing events, or establishing attribution.

5.1 Modern Anti-Forensic Methodologies

Encryption represents another major challenge for investigators. Strong cryptographic algorithms protect sensitive information by converting readable data into ciphertext that cannot be interpreted without appropriate decryption keys. Full-disk encryption, encrypted messaging platforms, virtual private networks, and encrypted cloud storage services have become increasingly common in both personal and organizational environments. While encryption provides essential security benefits, it can also prevent investigators from accessing potentially critical evidence. In some cases, investigators must rely on memory forensics, key recovery techniques, or legal mechanisms to obtain access to encrypted information.

5.2 The Privacy

The growing emphasis on privacy and data protection has introduced significant challenges for digital forensic investigations. Individuals, organizations, and governments increasingly demand stronger safeguards for personal information in response to rising concerns regarding surveillance, data breaches, and unauthorized access. As a result, technology providers have implemented sophisticated privacy-enhancing mechanisms that limit access to digital information.

From a forensic perspective, however, zero-knowledge frameworks create substantial investigative obstacles. Even when investigators obtain legal authorization to access information, service providers may be technically incapable of decrypting user data. Consequently, traditional evidence acquisition approaches become ineffective. Investigators may instead need to rely on endpoint devices, memory analysis, metadata examination, or alternative intelligence sources to reconstruct relevant activities.

VI Gaps and Vulnerabilities

Despite significant advancements in digital forensic technologies, numerous methodological, technical, and legal challenges continue to limit the effectiveness of contemporary investigations. The rapid evolution of digital ecosystems has outpaced the development of standardized forensic procedures, creating inconsistencies in evidence acquisition, analysis, interpretation, and presentation. Furthermore, emerging technologies such as cloud computing, artificial intelligence, blockchain systems, and Internet of Things (IoT) infrastructures have introduced complexities that traditional forensic frameworks were not designed to address.

6.1 The Standardization issues

One of the most persistent challenges facing digital forensics is the lack of global standardization. Digital investigations frequently involve data distributed across multiple countries, cloud providers, and legal jurisdictions. Differences in laws, regulations, evidence handling procedures, and privacy requirements create significant barriers to effective international cooperation.

Many countries have established their own forensic guidelines and legal frameworks governing digital evidence. While these frameworks often share common principles, substantial differences exist regarding evidence collection authority, admissibility

requirements, privacy protections, and cross-border data access. Such inconsistencies can delay investigations and create legal uncertainty.

6.2 Technical Bottlenecks

The exponential growth of digital data represents one of the most significant technical challenges confronting forensic practitioners. Modern organizations generate vast quantities of information through enterprise systems, cloud services, IoT devices, communication platforms, and security monitoring tools. Processing such datasets using conventional forensic techniques often requires substantial computational resources and lengthy analysis periods.

High-velocity data streams present an additional challenge. Modern systems continuously generate logs, network traffic records, sensor measurements, and application events. Capturing and preserving this information in real time requires scalable acquisition infrastructures capable of handling rapid data generation without compromising forensic integrity.

Future forensic systems must prioritize automation, parallel processing, intelligent filtering, and adaptive evidence management strategies. Such innovations will be essential for enabling timely investigations within increasingly data-intensive environments.

VII Next-Generation Investigative Framework

The future of digital forensics will be shaped by technological innovation, interdisciplinary collaboration, and evolving legal frameworks. As digital ecosystems continue to expand, investigators must adopt increasingly sophisticated methodologies capable of addressing emerging threats and complex evidence environments.

Cloud-native forensic platforms represent another promising area of development. These systems will enable investigators to acquire, process, and analyze evidence directly within distributed cloud environments. Such capabilities will be essential for addressing the increasing prevalence of cloud-based infrastructures and remote computing resources.

VIII. Conclusion

Digital forensics has evolved from a specialized discipline focused primarily on computer systems into a multidisciplinary field encompassing cloud infrastructures, Internet of Things environments, blockchain technologies, artificial intelligence systems, and decentralized digital ecosystems. This transformation reflects the increasing complexity of modern computing environments and the growing importance of digital evidence in criminal investigations, cybersecurity operations, corporate governance, and judicial proceedings.

As digital technologies continue to evolve, the field of digital forensics must remain adaptive and innovative to ensure the effective identification, preservation, analysis, and presentation of digital evidence in an increasingly interconnected world.

References

[1] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 4th ed. London, U.K.: Academic Press, 2020.

[2] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response,"

National Institute of Standards and Technology (NIST), Special Publication 800-86, 2019.

[3] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation*, vol. 7, pp. S64-S73, 2018.

[4] M. Scanlon and K.-K. R. Choo, "Cloud storage forensics," *Future Generation Computer Systems*, vol. 29, no. 2, pp. 673-681, 2018.

[5] R. Quick and K.-K. R. Choo, "Big forensic data reduction: Digital forensic images and electronic evidence," *Cluster Computing*, vol. 21, no. 2, pp. 723-740, 2019.

[6] R. van Baar, H. van Beek, and E. van Eijk, "Digital forensics as a service: A game changer," *Digital Investigation*, vol. 11, no. 1, pp. 54-62, 2019.

[7] M. Kohn, M. Eloff, and J. Eloff, "Integrated digital forensic process model," *Computers & Security*, vol. 38, pp. 103-115, 2020.

[8] A. Pichan, M. Lazarescu, and S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," *Digital Investigation*, vol. 26, pp. 77-96, 2020.

[9] N. Zawoad and R. Hasan, "FAIoT: Towards building a forensics aware ecosystem for the Internet of Things," *IEEE International Conference on Services Computing*, pp. 279-284, 2019.

[10] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416-3452, 2020.

[11] F. Breitinger, I. Baggili, and A. Marrington, "Research perspectives in digital forensics," *Digital Investigation*, vol. 10, no. 2, pp. 1-11, 2021.

[12] I. Baggili, A. T. Marrington, J. Liu, and K. Jones, "Advances and challenges in digital forensics," *Forensic Science International: Digital Investigation*, vol. 42, pp. 1-12, 2022.

[13] A. Alsmadi and A. Alshabanah, "Artificial Intelligence and Machine Learning in Digital Forensics: Current State and Future Directions," *IEEE Access*, vol. 11, pp. 55321-55345, 2023.

[14] Y. Mirsky and W. Lee, "The creation and detection of deepfakes: A survey," *ACM Computing Surveys*, vol. 54, no. 1, pp. 1-41, 2022.

[15] ENISA, "Electronic Evidence and Digital Forensics Challenges in Cloud Environments," European Union Agency for Cybersecurity, 2023.

[16] Maturi, S. Y. (2022). Vulnerabilities in the 802.11 wireless client selection mechanism. International Journal on Recent and Innovation Trends in Computing and Communication, 10(1), 106–117

[17] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).