International Organization of Research & Development (IORD)
ISSN: 2348-0831
Vol 13 Special Issue 02 | 2026

Cyber Security Challenges & Digital Forensic Solution in Modern System

Prof. Vaishnavi L. Tohare[1], Prof. Anshul A. Kukade[2], Prof. Vaishnavi J. Rathi[3]
[1,2,3] *Assistant Professor, Computer Science & Engineering, Siddhivinayak Technical Campus, Shegaon, Maharashtra, India*

DOI: 10.5281/zenodo.19539753

ABSTRACT

The accelerating digital transformation, characterized by the proliferation of interconnected devices and exponential data growth, has expanded the cyber-attack surface, giving rise to sophisticated threats that challenge traditional security measures and compel a paradigm shift in digital forensics. This paper provides a comprehensive overview of the predominant cybersecurity challenges confronting modern systems—including the volatility of evidence in cloud and IoT environments, the use of encryption and anti-forensic tactics by adversaries, and the scalability issues posed by big data. It critically examines the corresponding digital forensic solutions developed to mitigate these challenges. In response, we synthesize contemporary forensic methodologies, highlighting a decisive move towards the integration of Artificial Intelligence (AI) and Machine Learning (ML) for real-time threat analysis and automated evidence processing, alongside novel architectural paradigms like dew computing and hardware-accelerated forensics to facilitate real-time analysis at scale. By synthesizing current research, this paper aims to provide a structured understanding of the evolving relationship between cybersecurity threats and forensic methodologies, concluding with an identification of persistent research gaps to foster a more resilient and proactive approach to digital investigations in an increasingly hostile cyber landscape.

Keywords: - Cybersecurity Challenges, Digital Forensics, Cloud Forensics, IoT Security, Artificial Intelligence, Machine Learning, Anti-Forensics, Evidence Integrity, Dew Computing, Incident Response.

1. INTRODUCTION

The rapid growth in cybercrime and the increasing applicability of digital devices to traditional criminal investigation have made digital forensics an indispensable field in modern cybersecurity [1]. According to the International Telecommunication Union, global internet usage reached 5.4 billion people in 2023, accounting for approximately 67% of the world's population [1]. Complementing this, Cisco's Annual Internet Report indicates that by the end of 2023, total network-connected devices reached 29.3 billion, with network traffic averaging nearly 50 GB per user per month [1]. This digital symbiosis drives innovation but simultaneously presents unprecedented challenges for cybersecurity and digital forensics.

Digital forensics is a specialized field focused on identifying digital evidence and devices storing data digitally, using validated processes for legal applications both within and outside of a courtroom [1]. As organizations increasingly rely on interconnected systems, the potential for security breaches grows exponentially. Traditional digital forensic approaches were designed for standalone systems and static networks, making them inadequate for today's fluid and decentralized ecosystems comprising cloud platforms, IoT devices, mobile technologies, and multimedia systems [1][2].

The multifaceted nature of modern cyber threats demands a comprehensive approach to digital forensics that spans multiple domains. The escalation of cyber threats has been met with the development of sophisticated forensic tools such as Wireshark, Snort, Tcpdump, and Capsa, which play pivotal roles in capturing and analysing digital evidence [1]. These tools provide critical insights into cyber-attacks, aiding investigators in reconstructing the digital transmission chain and understanding attacker methodologies. However, the landscape continues to evolve, with adversaries developing increasingly sophisticated anti-forensic techniques to conceal their activities [3].

This paper addresses three fundamental research questions:

1. What are the primary challenges associated with digital forensics across different subdomains?
2. How do existing tools, frameworks, and methodologies address these challenges, and what are their limitations?
3. What research gaps exist in digital forensics, and what directions can future studies explore to enhance the field's efficacy and relevance?

2. BACKGROUND AND RELATED WORK

2.1 Evolution of Digital Forensics

Digital forensics has evolved significantly over the past decade, expanding from traditional computer forensics to encompass diverse subdomains including network, mobile, database, IoT, cloud, and multimedia forensics [1][2]. This evolution has been driven by the proliferation of digital devices and the increasing sophistication of cyber threats. The field now requires a holistic approach that integrates methodologies from multiple disciplines to effectively investigate cybercrimes [1].

Digital forensics plays a crucial role in securing, protecting, and monitoring network investigations, aiding investigators in navigating high-volume data to uncover pertinent evidence [1]. Digital evidence can emanate from various devices electronically connected to a network, including those under examination and those in smart environments. Filesystem directories offer access to low-level data, enabling investigators to trace machine activity and interpret how and where a device has been used previously [1].

2.2 The Current Threat Landscape

The cybersecurity threat landscape is constantly evolving, with cybercriminals continuously adapting their tactics and techniques to evade detection [3]. Global statistics paint a concerning picture:

- 5.4 billion internet users worldwide (67% of global population) [1]
- 29.3 billion network-connected devices [1]
- 50 GB average monthly network traffic per user [1]
- Expected 55.7 billion IoT devices by 2025 [4]

This massive attack surface creates unprecedented challenges for digital forensic investigators. Smart environments may hold collaborative data associated with multiple devices and evidence not locally saved on the machine, further complicating investigations [1].

2.3 Related Surveys and Studies

Previous research has made significant contributions to understanding digital forensics challenges. A comprehensive systematic literature review by [1] examined digital forensics across multiple subdomains, identifying process redundancies and ambiguities. The study proposed a high-level theoretical metamodel that unifies tasks, operations, procedures, and methods across subdomains to help forensic investigators organize and integrate evidence.

Research on anti-forensic techniques has categorized these methods into four distinct groups: artifact wiping, data hiding, trail obfuscation, and attacks against forensic tools [3]. Several studies have demonstrated the unreliability of current digital forensic tools in effectively countering anti-forensic techniques, highlighting the need for more robust and adaptive approaches [3].

Studies on IoT security have revealed the vulnerabilities inherent in resource-constrained devices that depend on communication across edge, fog, and cloud layers [4]. The integration of AI and ML into intrusion detection systems has emerged as a promising approach to addressing these vulnerabilities [4][5].

3. CYBERSECURITY CHALLENGES IN MODERN SYSTEMS

3.1 Evolving Digital Ecosystems and Data Complexity

Modern digital ecosystems are characterized by unprecedented complexity and decentralization. Multiple data input sources create massive volumes of data, making it difficult to access or trace breach sources [1]. The distribution of data across platforms compounds this challenge, as investigators must navigate disparate systems and formats to piece together evidence.

Table 1: Digital Forensics Challenges Across Domains

Domain	Key Challenges	Impact on Investigations
Network Forensics	High-volume traffic, encryption, real-time analysis	Difficulty in packet capture and analysis [1]
Mobile Forensics	Device fragmentation, encryption, frequent OS updates	Incomplete data acquisition [1]
Database Forensics	Large data volumes, transaction logs, live vs. static analysis	Complex reconstruction of events [1]
IoT Forensics	Device heterogeneity, resource constraints, distributed data	Evidence volatility and fragmentation [1][4]
Cloud Forensics	Multi-tenancy, jurisdiction issues, lack of physical access	Evidence acquisition challenges [1]
Multimedia Forensics	Deep fakes, manipulation detection, authenticity verification	Evidence reliability concerns [1]

3.2 Sophisticated Cyber Threats

Advanced Persistent Threats (APTs): APTs represent a significant challenge to organizational security. These sophisticated, long-term campaigns are designed to steal data or monitor activities over extended periods. APTs often employ multiple attack vectors and adapt their techniques to avoid detection, making them particularly difficult to investigate using traditional forensic methods [3].

Ransomware and Malware Evolution: Ransomware attacks have evolved from simple file encryption to sophisticated operations involving data theft and double-extortion tactics. File-less malware techniques allow attackers to operate "living off the land," using legitimate system tools to carry out malicious activities while leaving minimal forensic traces [3].

AI-Powered Attacks: The democratization of AI has enabled cybercriminals to launch more sophisticated attacks [5]. Deepfakes, automated social engineering campaigns, and voice synthesis for impersonation represent emerging threats that challenge both detection and investigation capabilities [1][5].

3.3 Anti-Forensic Tactics

Anti-forensics (AF) encompasses techniques and tools employed by cybercriminals to hinder or manipulate digital forensic investigations [3]. Research has identified four primary categories of anti-forensic techniques:

- **Artifact Wiping:** Permanently deleting or overwriting digital evidence to prevent recovery
- **Data Hiding:** Concealing data through steganography, encryption, or storage locations
- **Trail Obfuscation:** Creating misleading evidence or manipulating timestamps to confuse investigators
- **Attacks Against Tools:** Exploiting vulnerabilities in forensic software to compromise investigation integrity

Anti-forensic methods aim to frustrate forensic efforts at all stages, including evidence acquisition, examination, analysis, and reporting [3]. Malicious actors attack the three main constraints of forensic investigations: time, cost, and resources, potentially delaying or preventing investigations entirely [3].

3.4 Encryption and Cloud Complexities

The widespread adoption of encryption across devices, communications, and storage means that investigators often encounter encrypted data that cannot be easily accessed [3]. This "going dark" problem is compounded by end-to-end encryption in messaging applications, full-disk encryption on mobile devices, encrypted network protocols, and privacy-enhancing technologies.

Cloud computing introduces unique forensic challenges due to its distributed nature and multi-tenancy architecture [1].

3.5 IoT Security Vulnerabilities

The rapid expansion of IoT has introduced complex security challenges due to constrained devices and layered communication architectures [4]. IoT devices, often limited in computational power, storage, and battery capacity, depend on communication across edge, fog, and cloud layers, creating vulnerabilities that attackers can exploit [4].

Table 2: IoT Security Challenges Across Architectural Layers

Layer	Security Challenges	Forensic Implications
Edge Layer	Limited computational power, energy constraints, physical security	Minimal logging capability, evidence loss on power cycle [4]
Fog Layer	Distributed architecture, heterogeneity, latency requirements	Fragmented evidence across nodes [4]
Cloud Layer	Scalability, multi-tenancy, API security	Access restrictions, jurisdictional issues [4]

3.6 Scalability and Skills Gap

Existing forensic tools struggle with immense scalability issues posed by big data, including petabyte-scale data stores, high-velocity data streams, diverse data formats, and real-time investigation requirements [1][2]. According to the 2024 ISC2 Cybersecurity Workforce Study, there is a global shortage of 4.8 million cybersecurity workers, up 19% from the previous year. Digital forensics and incident response roles are particularly hard to fill due to highly specialized skill requirements, rapid technological changes, limited formal education programs, and high-stress nature of the job.

4. DIGITAL FORENSIC SOLUTIONS AND METHODOLOGIES

4.1 AI and Machine Learning Integration

Artificial Intelligence and Machine Learning are transforming digital forensics by enabling automated analysis at scale [5]. A comprehensive review of AI applications in digital forensics categorizes AI techniques into machine learning, symbolic AI, and hybrid systems [5].

4.1.1 Applications of AI in Digital Forensics

Table 3: AI/ML Applications in Forensics

Application Area	AI/ML Techniques	Benefits
Anomaly Detection	Deep Learning, Neural Networks	Real-time threat identification [4][5]
Forensic Triage	Classification Algorithms	Prioritization of evidence [5]
Behavioural Profiling	Pattern Recognition	User activity analysis [5]
Multimedia Analysis	Computer Vision, Deep Learning	Deep fake detection [1][5]

AI-Powered Forensic Frameworks: Several notable AI-powered frameworks have been developed including the D4I Framework which improves inspection and analysis stages by categorizing digital artifacts and relating them to Cyber-Kill-Chain assault phases, Fronesis focusing on explainable AI for forensic applications, and AIFIS for automated evidence processing [5][6].
Challenges in AI Adoption: Despite its promise, AI adoption faces challenges including explainability requiring explainable AI frameworks for legal admissibility, adversarial robustness against attacks targeting AI models, ethical concerns regarding privacy and bias, and validation needs for real-world benchmarking [5].

4.2 Cloud and IoT Forensics Solutions

Modern cloud forensics platforms have evolved to address unique challenges with capabilities including data enrichment through automated correlation with threat intelligence feeds, unified timeline view across various cloud platforms, saved searches for re-execution, faceted search for quick insights, and cross-cloud investigations [1].
IoT forensics requires specialized approaches due to device constraints and distributed architectures [4][6]. Intelligent IDS solutions utilizing AI, ML, and DL address protocol heterogeneity, computational complexity constraints, energy efficiency requirements, and real-time detection capabilities [4]. A multi-layered approach integrates edge layer for local evidence collection, fog layer for distributed processing, and cloud layer for centralized storage and deep analysis [4].

4.3 Dew Computing for Enhanced Forensics

Dew computing represents an emerging paradigm that integrates local computing capabilities with cloud resources to create a hybrid framework enhancing data security and forensic analysis [2]. By allowing devices to operate independently of constant internet connectivity, dew computing addresses significant challenges faced by traditional cloud computing architectures [2].
Key Benefits of Dew Computing:

- Real-time data processing enabling immediate analysis at the edge [2]
- Reduced latency minimizing dependence on cloud connectivity [2]
- Enhanced evidence integrity through local storage reducing transmission vulnerabilities [2]
- Improved data accessibility even without internet connection [2]

4.4 Countering Anti-Forensic Techniques

Addressing anti-forensic tactics requires a multi-faceted approach combining preventive measures, enhanced detection capabilities, and robust investigative methodologies [3]. Preventive strategies include proactive monitoring for continuous surveillance, enhanced logging with comprehensive audit trails, integrity checking through regular verification, and redundancy using multiple evidence sources. Detection techniques include memory forensics for identifying file-less malware, timeline analysis for detecting timestamp manipulation, steganalysis for uncovering hidden data, and tool validation for forensic software integrity [3].

4.5 Advanced Tools and Standardization

SPECTRE is a modular cyber incident response system designed for memory forensics offering snapshot processing and emulation capabilities, comparison and threat reporting functionalities, compatibility with widely used DFIR tools, anomaly detection, and integration with threat intelligence tools. Hardware-accelerated forensics using programmable hardware enables line-rate analysis to mitigate threats at scale.
Recent research explores Large Language Models (LLMs) for automating evidence analysis and documentation, improving investigation efficiency, enhancing traceability, and alleviating technical and judicial barriers [7]. A unified forensic metamodel has been proposed to organize and integrate evidence across domains, standardize procedures, and facilitate cross-domain collaboration [1]. Regulatory frameworks like NIS-2 Directive (2022) and BSI IT Forensic Guide (2011) influence digital forensics, though tensions exist between forensic integrity and cybersecurity regulation [8].

5. DISCUSSION AND FUTURE DIRECTIONS

5.1 Persistent Research Gaps

Despite significant advances, several research gaps persist in digital forensics [1][3][5]:

Table 4: Research Gaps in Digital Forensics

Research Gap	Description	Priority
Standardized Frameworks	Lack of unified approaches across jurisdictions	High [1]
Anti-Forensic Countermeasures	Need for robust defences against evolving AF techniques	High [3]
AI Explainability	Requirement for explainable AI in legal contexts	High [5]
Real-World Validation	Insufficient validation of frameworks in operational settings	Medium [5]
Privacy-Preserving Forensics	Balancing investigation needs with data protection	Medium [5]

5.2 Emerging Technologies and Future Directions

Neuromorphic Computing: Neuromorphic computing offers potential for ultra-fast intrusion detection in IoT environments by mimicking neural architectures for efficient processing [4]. Future research should explore energy-efficient forensic processing at the edge, real-time pattern recognition capabilities, and hardware-level security monitoring.

Federated Learning for Privacy-Preserving Forensics: Federated learning enables collaborative threat analysis across distributed nodes while preserving data privacy [4]. Applications include cross-organizational threat intelligence sharing, privacy-compliant evidence correlation, and distributed model training without data centralization.

Self-Evolving AI Systems: Self-evolving AI-driven IDS that adapt to new threats without human intervention represent a promising direction [4]. These systems would continuously learn from emerging attack patterns, automatically update detection capabilities, and reduce response times to novel threats.

Blockchain for Evidence Integrity: Blockchain technology offers potential solutions for maintaining evidence integrity throughout the forensic process through immutable chain of custody records, distributed evidence verification, and tamper-evident audit trails.

Explainable AI (XAI) for Forensics: The development of explainable AI frameworks is critical for ensuring legal admissibility of AI-generated evidence [4][5]. XAI in forensics should provide clear rationales for AI decisions, traceable evidence analysis paths, and human-understandable explanations.

5.3 Recommendations for Practitioners

Based on the findings of this review, we offer the following recommendations for digital forensic practitioners:

1. **Adopt Multi-Layered Approaches:** Implement forensic capabilities across edge, fog, and cloud layers to address the distributed nature of modern systems [4]
2. **Invest in AI-Augmented Tools**: Leverage AI/ML for automated evidence processing and analysis to handle scalability challenges [5]
3. **Develop Anti-Forensic Awareness:** Train investigators to recognize and counter anti-forensic techniques through continuous education [3]
4. **Establish Standardized Procedures:** Adopt unified frameworks for cross-domain investigations to ensure consistency and reliability [1]
5. **Prioritize Evidence Integrity:** Implement blockchain or similar technologies for maintaining chain of custody throughout investigations [1]
6. **Engage in Continuous Learning:** Stay updated on emerging threats and forensic technologies through professional development and research participation

5.4 Future Research Directions

The field offers numerous opportunities including development of open benchmarks for evaluating forensic tools, adversarially resilient AI models resistant to manipulation, privacy-preserving architectures respecting data protection regulations, cross-jurisdictional frameworks for global cooperation, and SME-focused solutions for organizations with limited resources [1][5][8].

6. CONCLUSIONS

The accelerating digital transformation has fundamentally expanded the cyber-attack surface, creating unprecedented challenges for cybersecurity and digital forensics. This paper has examined the evolving threat landscape, identifying key challenges including evidence volatility in cloud and IoT environments, sophisticated encryption and anti-forensic tactics, and scalability issues stemming from exponential data growth [1][2][3][4].

Contemporary digital forensic solutions are leveraging Artificial Intelligence and Machine Learning for automated evidence processing and real-time threat analysis, marking a decisive shift from reactive investigation toward proactive prevention [5]. Novel paradigms such as dew computing and frameworks like D4I offer promising approaches for addressing resource constraints and cross-domain investigation complexities [2][6].

However, significant challenges persist. The integration of AI raises critical concerns regarding explainability, adversarial robustness, and legal admissibility of automated evidence [5]. The intensifying arms race with cybercriminals employing anti-forensic techniques demands continuous evolution of countermeasures [3]. Furthermore, the global shortage of 4.8 million cybersecurity professionals compounds these technical challenges.

Future research must prioritize: (1) standardized forensic frameworks across jurisdictions, (2) robust anti-forensic countermeasures, (3) privacy-preserving forensic architectures, and (4) emerging technologies including neuromorphic computing, federated learning, and blockchain for enhanced evidence integrity [1][3][4][5].

In conclusion, by embracing technological innovations while maintaining scientific rigor and legal compliance, the digital forensics community can build more resilient approaches to combating cybercrime in an increasingly hostile digital landscape.

7. ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the management and principal of Siddhivinayak Technical Campus, Shegaon, for providing the necessary infrastructure and continuous encouragement to carry out this research work. We extend our heartfelt thanks to the Head of the Department, Computer Science & Engineering, for their valuable guidance and support throughout this study. The authors gratefully acknowledge the contributions of their colleagues and faculty members whose insightful discussions and constructive feedback significantly enhanced the quality of this paper.

8. REFERENCES

[1] "Unveiling cybersecurity mysteries: A comprehensive survey on digital forensics trends, threats, and solutions in network security," *ScienceDirect*, 2025. [Online]. Available: ScienceDirect.com [Accessed: 2026].
[2] "Exploring the Role of Dew Computing in Enhancing Cybersecurity and Digital Forensics: A Systematic Literature Review," *IEEE Xplore*, 2025. [Online]. Available: IEEE Xplore [Accessed: 2026].
[3] "Countering anti-forensic tactics in cybercrime investigations – a systematic literature review," *International Journal of Information Security*, vol. 24, article 210, Springer, 2025. [Online]. Available: SpringerLink [Accessed: 2026].
[4] "Unveiling IoT ecosystem security: A review of intelligent IDS, trends, challenges, and future directions," *ScienceDirect*, 2025. [Online]. Available: ScienceDirect.com [Accessed: 2026].
[5] "Artificial Intelligence in Digital Forensics: A Review of Cyber-Attack Detection Models and Frameworks," *Journal of Information Systems Engineering and Management*, 2025. [Online]. Available: jisem-journal.com [Accessed: 2026].
[6] S. Chatterjee, S. Satpathy, and P. K. Swain, "Digital Forensics Analysis on the Internet of Things and Assessment of Cyberattacks," *Wiley Online Library*, 2025. [Online]. Available: Wiley Online Library [Accessed: 2026].
[7] "Open Access Publications," *Universität Augsburg*, 2025. [Online]. Available: opus.bibliothek.uni-augsburg.de [Accessed: 2026].
[8] F. Weijers, "IT Forensic Challenges and Comparative Insights: A Comparative Analysis of the NIS-2 Framework (2022) with the BSI IT Forensic Guide (2011)," *GI Digital Library*, 2025. [Online]. Available: dl.gi.de [Accessed: 2026].