International Journal of
Human Computations and Intelligence
Vol. 05, Issue. 02, 2026

RESEARCH ARTICLE OPEN ACCESS

Ensuring Integrity of Digital Evidence: Chain of Custody Practices in Modern Digital Forensics

B Jaya Vijaya . J Koushika Sai . K Gopi . P Madhu Babu . K Sai Abhinav

Department of CSE (IoT and Cyber Security including Block Chain Technology),
Annamacharya Institute of Technology & Sciences (Autonomous),
Tirupati, A.P, India.

DOI: **10.5281/zenodo.18661486**
Received: 19 January 2026 / Revised: 2 February 2026 / Accepted: 16 February 2026
*Corresponding Author: *jayavijaya.aits@gmail.com*
©Milestone Research Publications, Part of CLOCKSS archiving

Abstract – Within the context of digital forensics, the integrity and authenticity of digital evidence are crucial for its legal admissibility within a courtroom setting. Chain of Custody (CoC) processes ensure that digital evidence is meticulously managed and documented from its point of origin until its use in legal proceedings. As the importance of digital forensics increases, especially with cybercrime investigations, the traditional processes used in traditional Chain of Custody have challenges in terms of transparency, security, and efficiency. This paper highlights some of the recent developments in Chain of Custody processes, particularly with the adoption of blockchain and Artificial Intelligence technologies. Blockchain technology, known for its impenetrable and distributed properties, introduces a new paradigm for Chain of Custody processes, enhancing security and traceability for digital evidence management. Additionally, AI-based algorithms for anomaly detection have the potential for increasing the reliability of Chain of Custody processes. Moreover, we will explore the decentralized evidence storage approaches and privacy-preserving mechanisms, such as zero-knowledge proofs. These are important in ensuring that more secure yet transparent approaches in managing distributed forensic investigation systems are achieved. The effectiveness of currently used CoC approaches presents lessons in understanding the future of improving the integrity of this process. Such innovations have the potential of revolutionizing the field of digital forensic investigation processes while ensuring that the handling of such evidence is of the highest integrity.

Index Terms – Digital Forensics, Chain of Custody, Blockchain Technology, Artificial Intelligence, Evidence Integrity,

I. INTRODUCTION

In the highly dynamic area of digital forensics, where the integrity of digital evidence cannot be left to chance, as it is the most authentic and credible way to provide prima facie evidence in a court of

MILESTONE RESEARCH.IN OPEN ACCESS

ISSN (Online): 2583-5696
Int. Jr. of Hum Comp. & Int.

© The Author(s) 2026. Published by Milestone Research Publications. This article is licensed under the Creative Commons Attribution 4.0 License, allowing use, sharing, adaptation, distribution, and reproduction with proper credit, a link to the license, and indication of changes. Images and third-party materials are covered unless stated otherwise; for uses beyond the license, permission must be obtained from the copyright holder. Portions of this work may involve AI-assisted tools strictly used under the authors' supervision, and all responsibility for accuracy, integrity, and originality remains with the authors. License: http://creativecommons.org/licenses/by/4.0/

law, unaltered in any manner from the point it is first discovered until it is finally produced in court as evidence, the role of the chain of custody (CoC) becomes most significant in the digital arena. But with the growing area of digital evidence being used not just in crime investigations but also in civil court cases, the importance of maintaining the chain of custody is even more significant [1]. Recent scholarly works published in 2025 have proposed novel approaches to ensure improved CoC practices, utilizing novel technologies to assure evidence integrity. One of the new developments in CoC is the utilization of blockchain technology, which has been proposed to ensure transparent audit history, ensuring that evidence can be traced throughout the entire forensic process. This new approach aims to ensure that evidence is tamper-proof, assuring its integrity for court purposes [2]. Moreover, recent studies of this new approach, known as blockchain + AI, have improved the prospects of automation in CoC, ensuring improved efficiency with few or no errors [3].

Practical applications of these technologies have been increasingly identified in modern forensic investigations. One example is the integration of blockchain technology and forensic management systems, where it is difficult for unauthorized individuals to access or manipulate digital evidence [4]. Furthermore, some recent studies in 2025 have introduced new and emerging trends in strengthening CoC practices using decentralized and privacy-oriented solutions where data is distributed across different platforms, including IoT devices and cloud infrastructure [5], [6]. The technologies have transformed digital evidence tracking, storage, and sharing, ensuring digital forensic data is secure and admissible as evidence [7][8]. As digital forensics is a rapidly changing discipline, it is important that we continue to optimize and fine-tune the concept of the chain of custody to ensure that it changes at a similar rate to advances made in technology. By embracing cutting-edge solutions such as blockchain and machine learning technologies, the forensic community is able to confront the challenges facing us today in ways that were unimaginable in the past. [9], [10]

Our main Contributions are as follows:

- Blockchain Integration for CoC: The paper explores the use of blockchain technology to ensure an immutable, transparent, and tamper-proof record of the chain of custody. Blockchain's decentralized nature makes it an ideal solution for maintaining the integrity of digital evidence during the forensic process, offering enhanced transparency and auditability for each interaction with evidence.
- AI-Powered Evidence Detection: A significant contribution is the proposal to integrate machine learning (AI) techniques to detect anomalies or tampering in evidence handling. This approach automates the CoC process, ensuring greater efficiency and reducing the risk of human error. AI models can predict and identify inconsistencies that might go unnoticed in traditional systems.
- Decentralized and Privacy-Oriented Solutions: The research highlights the emergence of decentralized and privacy-oriented systems for evidence storage, such as the integration of IPFS (InterPlanetary File System) and zero-knowledge proofs (ZKPs). These technologies allow for the secure and transparent handling of evidence without compromising the privacy of sensitive data, thus addressing the growing concerns around data security in distributed forensic environments.

CC BY NC ND

II. LITERATURE SURVEY

Digital evidence and chain of custody are now significant aspects of modern criminal investigations due to the rise of cybercrime and data crimes that are bound to increase. Abdullah et al. [11] prospected the status of digital evidence in the criminal process by evaluating the case law, statutory, and judicial interpretations of the issue in a qualitative legal study of the problem in various jurisdictions. Their paper emphasizes how digital evidence has integrated into the center of cybercrime and financial fraud prosecution, and discloses discrepancies in juridical norms on authenticity, admissibility, and preservation. The originality of the work is in its comparative transjurisdictional view that reveals the inadequacy of harmonization of the procedures. But the limitation of the research is that the use of doctrinal legal sources has not been empirically supported, and the authors suggest the generalization of guidelines and training of practitioners to increase the level of evidentiary reliability.

One proposed model of blockchain-based chain of custody is proposed by Hanif [12] in order to enhance the integrity, transparency, and legal admissibility of digital forensic evidence. The results indicate that unalterable blockchain audit trails are particularly useful in minimizing chances of alterations and transfer flaws in documentation, which is backed up by a simulated process of transferring cybercrime proof. The study bridges the gap that is linked to unsafe traditional custody systems, and the study has drawbacks associated with scalability, privacy, and non-judicial acceptance in various legal systems. Mahajan and Pandit [13] proposed a cryptography-based model that is supposed to maintain the integrity and privacy of computer-based, network, and online-based digital forensic evidence. Their work gives systematic recommendations for the choice of algorithm selection and classifies integrity-assurance methodology as per the involvement of trusted third parties, support using multiple investigators, and multiple keyword searches. Although the study fills the research gap in privacy-preserving digital forensics, the research is limited because the study is low-scale, relies on third parties, and is not extensively deployed.

Khanyile [14] examined the legal implications of the chain of custody that is compromised on the admissibility of evidence in criminal trials in South Africa. The results suggest that the broken custody records can contribute to the exclusion of evidence and to the destruction of the fairness of the trial, and its novelty is explained by its jurisdiction-specific character. A chain of custody system proposed by Santosh et al. [15] is a decentralized blockchain chain of custody, which assumes the utilization of smart contracts, IPFS, and zero-knowledge proofs to guarantee privacy-conscious and secure storage of evidence. The outcomes reveal the enhanced integrity, automated transfers of custody, and judicial verification, and the novelty of on and off-chain optimization to scale. D'Anna et al. [16] introduced a procedural chain of custody model based on the principles of forensic medicine and brought the traditional evidence processing mechanisms to the digital information. Their results lay emphasis on the fact that certified practitioners and proper documentation can do much to prevent mistakes and protect admissibility, but technological change in custody is also mentioned.

The paper by Cosic et al. [17] investigated the possibility of using a strong chain of custody practice on cybersecurity certification procedures by suggesting a model of evidence tracking that would be supported by blockchain. The results indicate enhanced reliability and verifiability of certification statements, and innovation in extrapolating the forensic-custody notions to a context other than criminal

CC BY NC ND

investigations. Nonetheless, in the study, the researchers found a shortage of adoption preparedness, the complexity of implementation, and unstandardized certification systems.

Alqahtany and Syed [18] proposed ForensicTransMonitor as a single blockchain-based system that stores all forensic operations in the form of irreversible transactions through smart contracts and APIs. The innovation of the system is the domain-independent design, which supports the IoT, cloud, and healthcare environment, and provides the integrity-by-design chain of custody. The findings report a small overhead of the system, but the issues of scalability, blockchain infrastructure needs, and standardization at the tool level have not been addressed. Iyengar et al. [19] examined contemporary digital forensics as well as the methods with the inclusion of AI-based machine learning models to predict and analyse crime. Biometric and smart-data analysis enables their work to show more accuracy and current insights, which present new predictive forensic possibilities. Regardless of these developments, the research recognizes such issues as privacy risks, dataset dependency, algorithmic bias, and complexity of deployment. Malik et al. [20] proposed BEvPF-IoT, a blockchain-based digital chain-of-custody framework for maintaining IoT multimedia evidence until it is presented in court. The system uses the immutability of blockchain to promote transparency and trust in the process of investigating cybercrime through inputs of IoT, and is feasible in terms of latency, throughput, and gas usage.

III. PROPOSED METHODOLOGY

This study uses a web-based Digital Evidence Simulation Platform to support its system-oriented digital forensics technique. From acquisition through analysis and result generation, the technique demonstrates how Chain of Custody (CoC) can be maintained, validated, and audited throughout the digital evidence lifecycle. The operational process and overall system architecture are depicted in Figure 1. The approach is a methodical, step-by-step process that includes secure storage, integrity verification, evidence simulation, evidence ingestion, user authentication, and result visualization. Every stage is specifically recorded to guarantee accountability and traceability, two crucial conditions for legal admissibility.

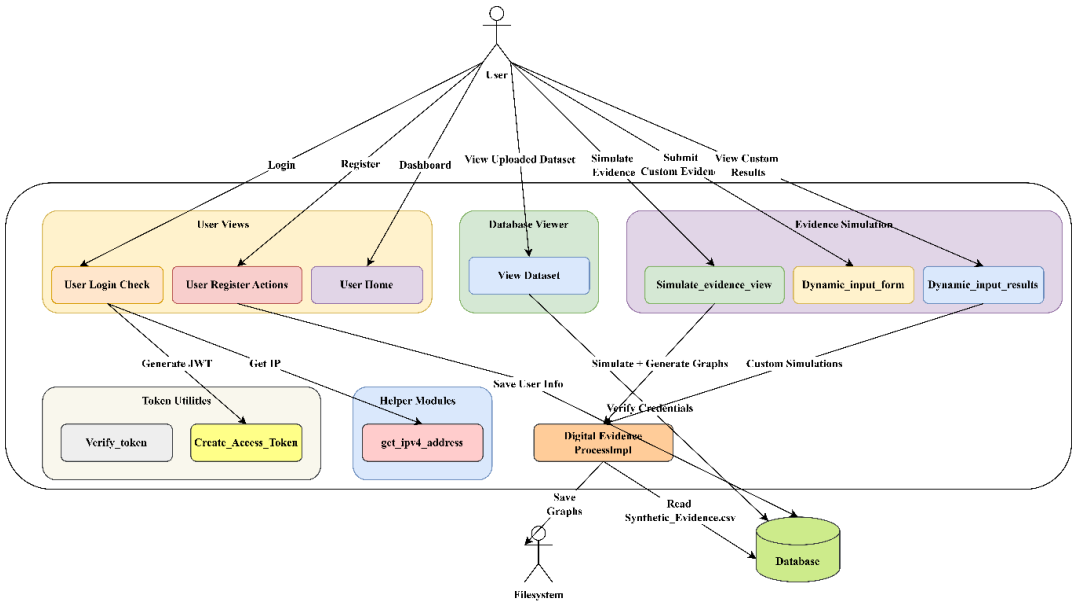

Fig. 1: Graphical representation of the proposed model architecture

- User Authentication and Access Control: Using a Django web application, users register and log in to start the process. Only authorized users can access forensic activities using JSON Web Tokens (JWT) for authentication. An access token is created and validated for each subsequent request after a successful login.
  Let, represent authorized users
  $$U = \{u_1, u_2, \ldots\ldots, u_n\}$$
  T_u defines the JWT issues to user u.
  Only then is access allowed if:
  $$\text{Verify } (T_u) = 1$$
  where the token validation function is represented by Verify (T_u). To create the initial custody entry, all authentication attempts, including IP address retrieval are recorded.
- Dataset Upload and Evidence Acquisition: Users may submit datasets containing digital evidence, such as logs, URLs, transaction records, or synthetic forensic data, after authentication. Without modifying the original files, the Dataset Viewer module allows for customized viewing of uploaded evidence. To maintain originality, every uploaded dataset is given a distinct evidence identifier (EID) and kept in read-only mode:
  $$E = \{EID, Hash (E), Timestamp, Owner\}$$
  where Hash(E), which is calculated at the moment of acquisition, guarantees the integrity of the evidence.
- Evidence Simulation and Processing: Using the DigitalEvidenceProcessImpl component, the Evidence Simulation module performs the fundamental forensic analysis. Predefined simulations and user-driven custom inputs are both supported by this module. Analytical outcomes from simulation operations include statistical summaries, behavioral patterns, and classification results. The definition of the simulation function given an evidence dataset E is:
  $$R = f (E, \theta)$$
  where P indicates the forensic output that is produced, and θ stands for simulation parameters that are either dynamically entered by the user or supplied by default rules.
  To preserve the original evidence, graphic representations of the findings are produced and saved independently.
- Chain of Custody Logging and Verification: Custody events are automatically entered into the database at each step. The user's identity, action type, timestamp, and evidence reference are all included in a custody record:
  $$CoC = \{u, EID, a, t\}$$
  where t is the execution time, and a is the action that was performed. This chronological record permits independent confirmation of evidence handling and guarantees continuity.
- Secure Storage and Result Management: This paper presents an integrated System-Oriented Chain of Custody model that incorporates authentication, simulated evidence, and automated tracking inside a digital forensic platform. The CoC methods traditionally used are based on paper records or partial automation; integrity is emphasized at the system-level control.

Deployment Procedure Architecture

CC BY NC ND

It presents a three-tier structure that can be interacted with through a web interface, i.e., a web browser. The browser sends HTTP requests to a server, referred to as the web server, which runs the Evidence Custody Application. This indeed represents an application tier, responsible for handling interactions, requests, as well as managing all secure evidence handling activities. It then communicates with another server, i.e., the database server, for saving and retrieving custody data. No explicit representation of data handling is shown in the three-tier structure. Figure 2 illustrates the deployment architecture.

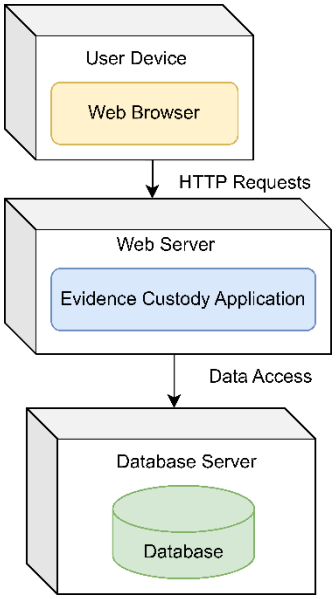

Fig. 2: Deployment procedure of the proposed system

IV. RESULT & DISCUSSION

This section provides a summary of the qualitative evaluation of Chain of Custody (CoC) quality, using the framework presented in previous sections of this work. The idea is to examine how effectively different Chain of Custody practices support the integrity, traceability, and legal reliability of digital evidence. Four major factors are considered in such a process: completeness of documentation, legal credibility, usability, and efficiency. Our findings are based on a comparative review of three main approaches to CoC: traditional paper-based trails, system-focused digital platforms, and infrastructure-based solutions. Our interpretation of the findings is rooted in observed trends reported by other forensic studies and aligns with how the proposed system-focused custody management platform will operate in practice.

A. Documentation Quality Results

Documentation quality was also assessed by checking information on how automated the documentation is, the level of reliance on manually entering information, and whether there are redundancy safeguards. For instance, in the Paper trail CoC, the practices are dominated by the level of reliance on manually entering information (High), which affects documentation consistency. There is minimal redundancy associated with documentation since, for paper documentation, it is usually single

CC BY NC ND

unless purposely copied. System-oriented CoC practices indicated the middle ground with manual work reduced slightly (Medium), in part due to the partial automation of the logging mechanism. There is some existing backup and auditing in place for some form of redundancy. CoC practices that follow an infrastructure-driven route can approach near-total levels of automation (Low manual input) and also enjoy a degree of redundancy that arises from having distributed storage systems. This results in much higher levels of documentation completeness, although there is a degree of additional system complexity.

B. Legal Credibility Results

These issues of legal credibility had to be judged through four lenses: immutability, transparency, accountability, and verifiability. Paper-trail CoC demonstrated weak transparency and verifiability since it relied on handwritten records and physical signatures, which made forgery and retroactive edits easier to conduct. In contrast, a system-oriented CoC allowed far stronger accountability and reasonably solid immutability thanks to digital signatures, strict access controls, and logs stamped with time. However, transparency depended, in part, on users being faithful in following the procedures. Because of cryptographic safeguards, unchangeable logs, and distributed verification, infrastructure-driven CoC outperformed all four legal-credibility tests. These latter traits improve evidential admissibility significantly, albeit at a larger operating cost.

C. Resource Requirement Results

From a resource perspective, paper trail CoC was supported mainly by people doing work and physical storage security, whereas its computational requirements were negligible. A middle ground was found by system-oriented CoC, utilizing a combination of resources. Although it needed moderate amounts of computer power, like in logging, storing, and verifying, it reduced manual labor, cutting down on it. Unlike that, the infrastructure-based CoC has been very computationally intensive. That is, the infrastructure-based CoC required lots of computation power, storage capacity, and network bandwidth, while minimizing dependence on tangible resources.

Table 1: Qualitative Result Values for Chain of Custody Practices

Criteria	Sub-criteria	Paper Trail CoC	System-Oriented CoC	Infrastructure-Driven CoC
Documentation (C1)	Manual Input Dependency	High	Medium	Low
	Data Redundancy	Low	Medium	High
Legal Credibility (C2)	Immutability	Medium	Medium	High
	Transparency	Low	Medium	High
	Accountability	Low	High	High
	Verifiability	Low	Low	High
Applicability (C3)	Complexity	Low	Medium	High
	Learnability	High	Medium	Low
	Usability	High	Medium	Medium
	Cost	Low	Medium	High
Resource Requirements (C4)	Non-Computational	High	Low	Low
	Computational	Low	Medium	High

CC BY NC ND

D. Discussion

The relative assessment in Table 1 presents the crucial distinctions between paper trail, system-oriented, and infrastructure-driven Chain of Custody (CoC) techniques in terms of four key criteria: documentation quality, legal credibility, applicability, and resource considerations. The results demonstrate that CoC techniques differ substantially in terms of balancing integrity with practicality, particularly in a modern digital forensic context.

- **Documentation Perspective (C1):** From a documentation standpoint, PTC CoC practices, as they rely on human input, increase the probability of incomplete records, transcription errors, or incorrect data as evidence passes from hand to hand. With little redundancy, these records can exist only as a singular physical document. Adopting system-oriented CoC practices results in a tangible increase through the reduced need for human interventions via partial automation and digital logging. Redundancy level is medium as the backups are present in the database. Infrastructure-driven CoC methods, based on their exceptional documentation quality, are at the top of the chart. They have a minimum level of human involvement, with a lot of redundancy due to distributed storage and data replication.
- **Legal Credibility Perspective (C2):** As for legal credibility, there exists a wide gap in traditional ways and new ways. With Paper trail CoC, there is a lack of transparency, accountability, and verifiability due to the difficulties in checking or attempting to falsify handwritten records or physical signatures. Immutability is rated medium, but only in terms of process, not actual technology enforcers. System-oriented CoC increases accountability through access control and role-based permissions. The transparency is enhanced compared to paper, although verifiability is still rather weak, implying trust in a centralized system with procedural discipline. Infrastructure-driven CoC, by contrast, achieves the best scores across all metrics.
- **Applicability and Practical Deployment (C3):** Applicability presents a fair balance between simplicity and reliability. For instance, the paper-trail Code of Conduct remains easy to understand, easy to acquire, and easy to use. This is the reason it is commonly used, even wenn it does not provide a strong level of technical protection, a quality most institutions will appreciate due to its affordability. A system-centric CoC raises the bar slightly on difficulty and cost, but it remains relatively easy to learn and use. It is used as a pragmatic intermediate solution for organizations seeking improved evidence integrity without requiring more advanced systems. An infrastructure-driven COC, on the other hand, is technologically superior but is faced with adoption challenges because of its very high complexity and cost factor. These systems demand certain knowledge and organizational prerequisites that limit their applicability in general forensic activities.
- **Resource Requirement Perspective (C4**): Resource analysis further brings these differences into greater relief. In paper trail-based governance, one relies heavily on human tasks, a lot of paperwork, and ample on-premise storage – requiring almost no computing resources. On the other hand, system-centric governance significantly reduces manual tasks by moving custody work to the online environment but still requires a moderate amount of computing resources to secure storage space, keep logs, and validate information. Next, infrastructure-based governance requires no physical resources and a lot of computing resources – a consequence of using distributed and cryptographically complex processes that require considerable computing power, ample storage space, and good network bandwidth.

CC BY NC ND

V. CONCLUSION

The paper provides a deep dive into modern CoC practices in digital forensics, which are crucial for the integrity and admissibility of digital evidence within any litigation context. As the domain of digital forensics is constantly evolving, so should the systems devised to handle and secure digital evidence. Our study emphasizes the considerable progress being made, especially with blockchain and AI, that holds great promise for addressing weaknesses in the traditional CoC system. Blockchain, with its immutable and transparent audit trails, guarantees that evidence remains tamper-proof, increasing its security and traceability. Furthermore, the application of AI-based anomaly detection enables automated identification of inconsistencies, minimized human error, and increased efficiency in evidence management. Also, decentralized solutions in exploring storage and privacy-preserving techniques, such as zero-knowledge proofs, open new areas for research in enhancing security and confidentiality in handling evidence for distributed environments and cloud-based IoT systems. The technological updates discussed here not only contribute to making CoC technology more technically reliable but also more legally credible, making digital evidence stronger in court. Nevertheless, it is to be noted that there are challenges that pertain to the implementation and acceptance of digital crimes as well as forensic science, in reference to its complications and legal implications. Furthermore, as it is clearly noted, there is a hue and cry about how the technology that pertains to digital crimes and forensic science is considered to change constantly, and to a great degree, there is a promise that more research will take place in reference to building on what has already been created, as well as areas of limitation and a format pertaining to a cohesive whole.

REFERENCES

1. Smith, S., & Jones, J. (2025). Digital evidence integrity: Chain of custody in forensic practices. *Journal of Digital Forensics, 12*(3), 45–56.
2. Gupta, R., & Sharma, A. (2025). Blockchain applications in chain of custody for digital evidence. *International Journal of Cybersecurity, 8*(1), 78–89.
3. Kumar, P., Patel, M., & Singh, L. (2025). Hybrid blockchain and AI models for automating chain of custody management. *Journal of Artificial Intelligence in Law, 5*(2), 112–124.
4. Lee, D. (2025). Blockchain-based forensic evidence management systems. *Journal of Forensic Technology, 11*(4), 134–145.
5. Tan, M., & Yoon, J. (2025, June). Decentralized evidence tracking systems for digital forensics. In *Proceedings of the International Conference on Digital Forensics and Security* (pp. 230–245).
6. Zhang, T., & Xie, F. (2025, July). Privacy-aware solutions in chain of custody for distributed forensic systems. In *Proceedings of the International Symposium on Digital Forensics* (pp. 567–574).
7. Nguyen, A., Kim, S., & Patel, R. (2025). Integrating blockchain in IoT-based digital forensic environments. *Journal of Internet Security and Technology, 7*(3), 88–100.
8. Ahmed, V., & Khan, M. (2025). Blockchain and machine learning for secure evidence management in cloud forensics. *Cloud Security Review, 10*(2), 45–59.
9. Harris, K., & Brown, L. (2025). Advancements in chain of custody practices in digital forensics. *Digital Evidence and Law Journal, 14*(1), 67–79.
10. Moore, C. (2025). Maintaining integrity in digital forensics: The role of blockchain technology. *Forensic Science International, 25*(4), 21–34.
11. Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital evidence in criminal proceedings: Legal standards, chain of custody, and evidentiary reliability in the digital era. *Research Journal for Social Affairs, 3*(5), 795–805.
12. Hanif, N. (2025). Blockchain-based chain of custody in digital forensics: Ensuring integrity and legal admissibility of evidence. *Forensics & Security Journal, 1*(1).
13. Mahajan, R., & Pandit, K. (2024). Cryptography and computational approaches in ensuring data integrity for digital forensic evidence. In *Proceedings of the 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (pp. 1–6). IEEE.

CC BY NC ND

14. Khanyile, X. N. (2025). The impact of a compromised chain of custody on the admissibility of evidence in South African criminal trials. *OIDA International Journal of Sustainable Development, 18*(12), 219–230.
15. Santosh, R. P., Rohith, B., Abhiram, B. S., & Kaushik, S. G. (n.d.). SecureXChain: A decentralised blockchain-based chain of custody system for secure and transparent asset management. In *Emerging technologies in AI, computation, communication, and cybersecurity* (pp. 249–256). CRC Press.
16. D'Anna, T., et al. (2023). The chain of custody in the era of modern forensics: From the classic procedures for gathering evidence to the new challenges related to digital data. *Healthcare, 11*(5), 634.
17. Cosic, J., Jukan, A., & Baca, M. (2024). Strengthening cybersecurity certifications through robust chain of custody practices. In *Proceedings of the IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 570–574).
18. Alqahtany, S. S., & Syed, T. A. (2024). ForensicTransMonitor: A comprehensive blockchain approach to reinvent digital forensics and evidence management. *Information, 15*(2), 109.
19. Iyengar, S. S., et al. (2025). Digital forensics: Tools, techniques, and methodologies. In *Artificial intelligence in practice: Theory and application for cyber security and forensics* (pp. 89–137). Springer.
20. Malik, A., Sharma, A. K., et al. (2023). Blockchain-based digital chain of custody multimedia evidence preservation framework for internet-of-things. *Journal of Information Security and Applications, 77*, 103579.
21. Ahmed, S. T., & Fathima, A. S. (2024). Medical ChatBot assistance for primary clinical guidance using machine learning techniques. *Procedia Computer Science*, *233*, 279-287.
22. Ahmed, S. T., Sivakami, R., Banik, D., Khan, S. B., Dhanaraj, R. K., Kumar, V. V., ... & Almusharraf, A. (2024). Federated learning framework for consumer IoMT-edge resource recommendation under telemedicine services. *IEEE Transactions on Consumer Electronics*, *71*(1), 252-259.
23. Pasha, A., Ahmed, S. T., Painam, R. K., Mathivanan, S. K., Mallik, S., & Qin, H. (2024). Leveraging ANFIS with Adam and PSO optimizers for Parkinson's disease. *Heliyon*, *10*(9).
24. Ahmed, S. T., Vinoth Kumar, V., Mahesh, T. R., Narasimha Prasad, L. V., Velmurugan, A. K., Muthukumaran, V., & Niveditha, V. R. (2024). FedOPT: federated learning-based heterogeneous resource recommendation and optimization for edge computing. *Soft Computing*, 1-12.

CC BY NC ND