International Research Journal of Education and Technology

Peer Reviewed Journal, **ISSN: 2581-7795**

INTEGRATED DIGITAL EVIDENCE CHAIN OF CUSTODY AND END TO END CYBER THREAT DETECTION AND RESPONSE FRAMEWORK

Ms. Raseetha K N, Mr. Ragul T G

III B.Sc. Digital and Cyber Forensic Science

Dr. A. Sherin, Associate Professor

Department of Digital and Cyber Forensic Science

Nehru Arts and Science College

Coimbatore

I. Abstract

The rapid growth of sophisticated cyber threats has created an urgent need for a unified framework that integrates digital forensic investigation with real-time threat detection and response mechanisms. This paper proposes an Integrated Digital Evidence Chain of Custody and End-to-End Cyber Threat Detection and Response Framework designed to ensure evidence integrity, accountability, and rapid incident mitigation. The framework combines automated threat intelligence, Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), network monitoring, and digital forensic acquisition tools into a centralized architecture. A key contribution of this study is the incorporation of a tamper-proof digital chain of custody model that maintains cryptographic hashing, timestamping, and secure logging to preserve evidentiary authenticity throughout the incident lifecycle. The framework ensures compliance with forensic standards while enabling proactive threat hunting, anomaly detection using machine learning techniques, and coordinated response automation.

Keywords: Digital Evidence , Chain of Custody , Cyber Threat Detection , Cybersecurity Framework , Threat Inteligenence , Evidence Integrity , Security Monitoring , SIEM.

II. Introduction

In the modern digital era, cyber threats have become increasingly sophisticated, frequent, and damaging to organizations across all sectors. The rapid growth of networked systems, cloud computing, Internet of Things (IoT), and mobile technologies has significantly expanded the attack surface, making traditional security approaches insufficient. Organizations not only need effective cyber threat detection and response mechanisms but also must ensure that digital evidence collected during incidents is properly preserved and legally admissible.An integrated digital evidence chain of custody combined with an end-to-end cyber threat detection and response framework provides a comprehensive solution to these challenges. The chain of custody ensures the integrity, authenticity, and traceability of digital evidence from the point of collection to presentation in legal or disciplinary proceedings.

III. Literature Survey

Digital forensics and cyber threat detection are important for identifying and investigating cyber attacks. The chain of custody ensures that digital evidence is properly collected, stored, and preserved without alteration. Recent research uses technologies like AI, machine learning, and blockchain to improve evidence security and threat detection. An integrated framework helps enhance investigation efficiency and response to cyber threats. Digital evidence plays a critical role in cybercrime investigations. Proper chain of custody (CoC) procedures ensure that digital evidence is collected, preserved, and documented without modification from the time of acquisition until presentation in court. Maintaining the integrity and authenticity of evidence is necessary for legal admissibility. Recent research highlights the need for improved digital evidence management systems that include audit logging, secure storage, and controlled access mechanisms to maintain evidence reliability during investigations.

IV. Methodology

The methodology follows an integrated approach combining cyber threat detection, incident response, and digital evidence chain of custody management. Initially, system logs, network traffic, and endpoint data are continuously collected and monitored through security tools. Detected threats are analyzed using signature-based and anomaly detection techniques**.**

1. Data Collection

Collect system logs, network traffic data, and security alerts from different sources such as servers, firewalls, and intrusion detection systems.

2. Threat Detection

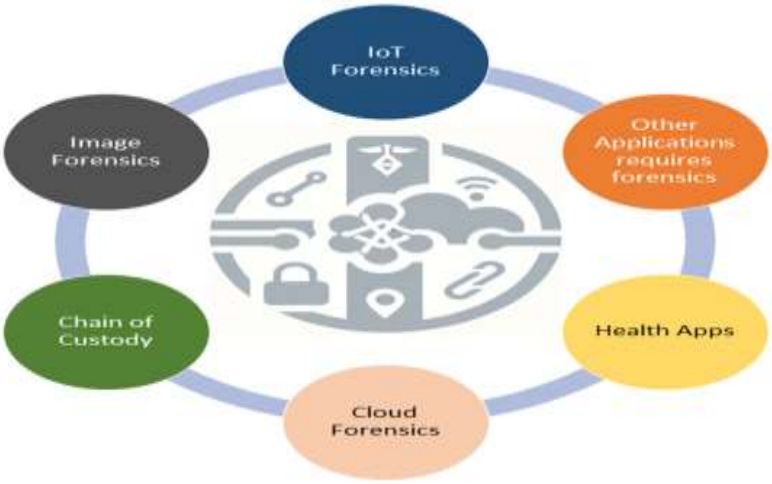
Analyze the collected data using security analysis techniques or machine learning models to identify suspicious activities or cyber threats.

3. Threat Detection

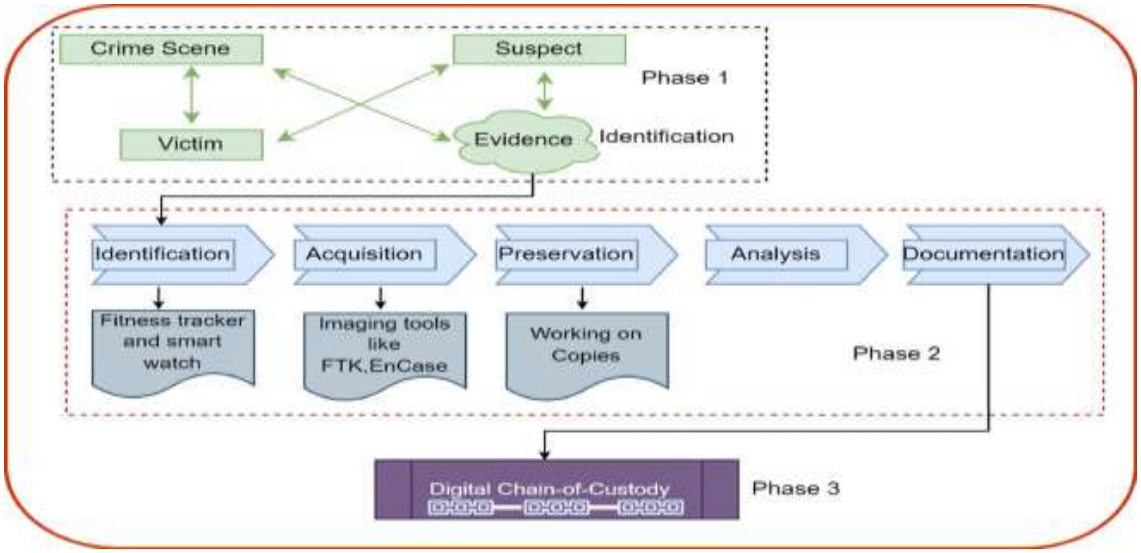
Take necessary response actions such as blocking malicious IPs, isolating infected systems, and applying security patches.

V. Architecture

The architecture for the “Integrated Digital Evidence Chain of Custody and End-to-End Cyber Threat Detection and Response Framework” consists of several interconnected layers that work together to detect cyber threats and securely manage digital evidence. This layer collects data from multiple sources such as system logs, network traffic, firewalls, intrusion detection systems, and user activities.



Overall Workflow:
Data Collection → Evidence Identification → Evidence Acquisition → Chain Of Custody Recording → Evidence Storage And Preservation → Threat Detection And Analysis → Incident Response And Mitigation → Reporting → Documentation



VII. Analysis of Problem

With the rapid growth of internet usage and digital technologies, cyber attacks and cybercrimes are increasing significantly. Organizations face challenges in detecting threats quickly and managing digital evidence properly during cyber investigations. Many existing systems focus only on threat detection but do not maintain a proper digital evidence chain of custody, which is necessary to ensure the integrity and authenticity of evidence.Another major problem is the lack of integration between cyber threat detection systems and digital forensic processes. Evidence collected during incidents may be altered, lost, or poorly documented, which can affect legal investigations. In addition, large volumes of data from networks and systems make it difficult to identify real threats efficiently.

Limitations of Existing System

Existing systems lack integration, rely on manual processes, have visibility gaps, respond slowly, and face compliance risks.

1. **Manual Evidence Handling**
   Many systems rely on manual documentation of digital evidence, which can lead to errors and data loss.
2. **Lack of Proper Chain of Custody**
   Existing systems do not always maintain a secure and traceable record of who accessed or handled the evidence.
3. **Delayed Threat Detection**
   Traditional security systems may detect cyber threats slowly, which increases the risk of damage.
4. **Poor Integration**
   Cyber threat detection tools and digital forensic systems often work separately, making investigations difficult.
5. **Data Integrity Issues**
   Digital evidence can be modified or tampered with due to weak security controls.
6. **Handling Large Data Volumes**
   Existing systems struggle to analyze large amounts of logs and network data efficiently.

VIII. Applications and Future Scope

The integrated digital evidence chain of custody and end-to-end cyber threat detection and response framework can be used in various areas such as cybercrime investigation, digital forensic analysis, and network security monitoring. It helps investigators securely collect, store, and manage digital evidence while maintaining proper documentation of the chain of custody. Law enforcement agencies and cybersecurity teams can use this framework to detect cyber threats, analyze security incidents, and respond effectively. It also supports organizations in protecting their systems, networks, and sensitive data from cyber attacks.

Future Scope

In the future, this framework can be improved by integrating advanced technologies such as artificial intelligence and machine learning to enhance cyber threat detection and automate incident response.

1. **Integration with Artificial Intelligence:** AI can improve threat detection accuracy and automate cyber incident response

2. **Blockchain for Chain of Custody:** Blockchain technology can provide tamper-proof records for digital evidence management.
3. **Cloud-based Security Systems:** Future systems can store and analyze evidence securely using cloud platforms.
4. **Real-time Threat Detection:** Advanced systems can detect and respond to cyber threats instantly.
5. **Improved Automation**: Automation can reduce manual work in evidence collection, analysis, and reporting.

VIII. Challenges

Implementing an integrated digital evidence chain of custody and end-to-end cyber threat detection and response framework involves several challenges. One major challenge is handling the large volume of data generated by networks, systems, and security devices, which makes threat detection and analysis difficult. Maintaining the integrity and authenticity of digital evidence during collection, storage, and analysis is also critical. Ensuring a proper chain of custody requires accurate documentation of every step in evidence handling, which can be complex. In addition, integrating different cybersecurity tools and forensic systems into a single framework is technically challenging. Real-time threat detection and quick incident response require advanced technologies and high processing capabilities, while maintaining data security and privacy.

X. Conclusion

The integrated digital evidence chain of custody and end-to-end cyber threat detection and response framework provides a comprehensive solution to modern cybersecurity challenges. By combining continuous threat monitoring, structured incident response, and forensically sound evidence handling, the framework ensures both operational efficiency and legal reliability. The integration enhances detection accuracy, reduces response time, and preserves the integrity and authenticity of digital evidence throughout the investigation lifecycle. Maintaining a documented chain of custody strengthens accountability and supports legal admissibility in judicial proceedings. Overall, the proposed framework improves organizational cyber resilience by bridging the gap between cybersecurity operations and digital forensics, enabling proactive defense, efficient incident management, and secure evidence preservation.

Reference

1. National Institute of Standards and Technology (NIST), Guide to Computer Security Log Management, NIST Special Publication 800-92, 2006.
2. National Institute of Standards and Technology (NIST), Computer Security Incident Handling Guide, NIST Special Publication 800-61 Rev. 2, 2012.
3. National Institute of Standards and Technology (NIST), Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86, 2006.
4. ISO/IEC 27037:2012, Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, International Organization for Standardization, 2012.

5. ISO/IEC 27043:2015, Incident Investigation Principles and Processes, International Organization for Standardization, 2015.
6. E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed., Academic Press, 2011.
7. K. Kent, S. Chevalier, T. Grance, and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, NIST SP 800-86, 2006.
8. M. Behl and S. Behl, "Cybersecurity and cyberwar: What everyone needs to know," Oxford University Press, 2016.
9. R. Grimes, Hacking the Hacker: Learn From the Experts Who Take Down Hackers, Wiley, 2017.
10. S. Mansfield-Devine, "Security information andU event management (SIEM): A practical guide," Network Security, vol. 2016, no. 9, pp. 5–8, 2016.
11. ENISA (European Union Agency for Cybersecurity), Digital Forensics – Tools and Methods for Evidence Collection, Preservation and Analysis, 2019.

Ragul T G (USN: 23UGDF030) is an aspiring professional with a strong interest in Digital and Cyber Forensic Science. He is passionate about exploring advanced techniques in cybercrime investigation, digital evidence analysis, and emerging security technologies with a keen focus on cybersecurity, forensic methodologies, and ethical digital practices, his aims to contribute to building a secure and trustworthy digital environment. He can be reached Ragulneka7@gmail.com or via mobile at 8428164337 for academic and research collaboration.

Raseetha K N (USN: 23UGDF031) is an aspiring professional specializing in Digital and Cyber Forensic Science. She is deeply passionate about exploring cybercrime investigation, digital evidence analysis, and emerging security technologies, with a strong focus on cybersecurity, forensic methodologies, and ethical digital practices. Raseetha aims to contribute to creating a secure and trustworthy digital ecosystem by leveraging advanced forensic techniques and research-driven approaches. She is actively seeking opportunities for academic and research collaboration, and can be reached at: Email: Raseethakrishnakumar@gmail.com Mobile: 8778865324