Blockchain-Enhanced Digital Forensics: The Convergence of Immutable Ledgers, AI Agents, and Semantic Knowledge Graphs

Madineni Navanath
Dept. of Computer Science and Engineering, NMAM Institute of Technology, NITTE (Deemed to be University)
Karkala, Udupi, India

P. Venkataramana Bhat
Dept. of Computer Science and Engineering, NMAM Institute of Technology, NITTE (Deemed to be University)
Karkala, Udupi, India

Abstract

The landscape of digital forensics is undergoing a seismic shift, driven by the proliferation of ubiquitous computing and the 'Zettabyte Era' of data generation. The era of 'dead box' forensics—analyzing static data from powered-off hard drives—has effectively ended. The discipline of digital forensics stands at a critical juncture, besieged by the exponential growth of digital evidence and the increasing sophistication of anti-forensic techniques. Contemporary investigations involving the Internet of Things (IoT), Industrial Control Systems (ICS), and automotive data are buckling under the weight of manual acquisition and centralized logging. This paper proposes a novel, comprehensive framework: Blockchain-Enhanced Digital Forensics (BEDF). We synthesize the immutable trust of Distributed Ledger Technology (DLT) with the high-throughput analytical capabilities of Artificial Intelligence (AI) and the semantic structure of Data-Information- Knowledge-Wisdom (DIKW) graphs. Unlike existing solutions that focus primarily on cryptocurrency tracking, BEDF addresses the internal Chain of Custody (CoC) for enterprise environments. We provide a rigorous formal threat model utilizing the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE) methodology to validate system resilience, detail specific Convolutional Neural Networks (CNN) / Long Short-Term Memory (LSTM) architectures for automated malware detection to ensure reproducibility, and offer a theoretical complexity analysis demonstrating the viability of Practical Byzantine Fault Tolerance (PBFT) consensus for high-velocity forensic logging.

Index Terms

Digital Forensics, Blockchain, Artificial Intelligence, Chain of Custody, DIKW Graph, Hyperledger Fabric, Threat Modeling, STRIDE, Consensus Complexity