IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303277 |

Judicial Evidence Integrity and Security System for Fair Judgement

Mohamed Faizal.S, Mohamed Sabeer.N, Thowfiq Aziz.H, Dr.S.Praveen Kumar,

UG Student, Dept. of CSE, E.G.S Pillay Engineering College, Nagapattinam, India

UG Student, Dept. of CSE, E.G.S Pillay Engineering College, Nagapattinam, India

UG Student, Dept. of CSE, E.G.S Pillay Engineering College, Nagapattinam, India

Assistant Professor, EGS Pillay Engineering College, Nagapatinam, India

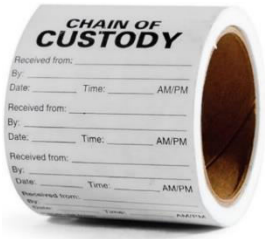
ABSTRACT: Digital evidence plays a vital role in investigations, being stored, received, or transmitted through electronic devices. It serves as the cornerstone for decision-making in criminal investigations, civil lawsuits, and regulatory compliance. However, maintaining the security and integrity of digital evidence faces challenges such as data alteration, unauthorized access, and flaws in centralized storage systems. Therefore, the development of a secure storage model is imperative to bolster the investigation process and safeguard sensitive information.To address the lack of an automated mechanism for preserving evidence and ensuring its integrity, a novel model has been devised. This model presents an efficient forensics architecture leveraging blockchain technology to establish a Chain of Custody (CoC) and employing Deep Learning Models for tamper detection. The proposed architecture involves stakeholders participating in a private network to collaborate on different investigation activities before storing them on the blockchain ledger. Tampering detection is facilitated using tailored deep learning algorithms for various file types, including Image with CNN, Word Document Embeddings using BERT, Video Frame-level Analysis with TCN, Audio Spectrogram Analysis with HMM, and PDF Document Structure Analysis.By utilizing fuzzy hash functions, forensic investigators can effectively manage permissible alterations of digital evidence, thereby standardizing forensic processes within the DB-CoC architecture. This standardized approach not only enhances result quality but also ensures robust information integrity, prevention, and preservation mechanisms. Consequently, the proposed architecture enables the permanent and immutable storage of evidence (chain of custody) in a private permissioned encrypted blockchain ledger.

KEYWORDS: Blockchain technology, digital forensic, deep learning, fuzzy hash function.

I. INTRODUCTION

A. OVERVIEW

The principle of Chain of Custody (COC) holds paramount importance within the legal sphere, ensuring the steadfast preservation of evidence's identity and integrity from its inception in the collection phase to the eventual disclosure of test outcomes. It encompasses the detailed documentation or trail of records that delineates the retrieval, custody, control, transfer, scrutiny, and disposal of evidence. Rigorous adherence to legal COC protocols during specimen acquisition is imperative to guarantee the dependability and integrity of subsequent analyses. Effectively recognizing, procuring, packaging, transmitting, scrutinizing, and preserving specimens substantially bolsters the admissibility of findings and enables sound expert interpretation within the judicial framework (Lyle 2004). According to the Evidence Act 1950, COC is further expounded as the witnessed, written records maintained by all individuals who have exercised uninterrupted control over the items of evidence.



| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

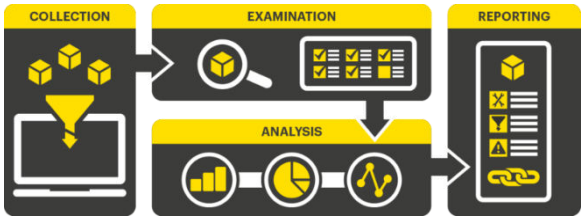
|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303277 |

Chain of Custody pertains to the documentation indispensable for establishing an exhaustive record detailing the oversight, transfer, and eventual disposition of evidence in criminal proceedings. This evidence may encompass DNA samples, photographs, documents, personal belongings, or bodily fluids either procured from a defendant or discovered at the scene of an alleged offense.

B. PROCESS OF A CHAIN OF CUSTODY FOR DIGITAL EVIDENCE

To safeguard digital evidence, the chain of custody entails four distinct phases:



- **Data Collection:**The examiner labels and documents each acquired item, noting its origin, collection method, timing, storage, and authorized access.
- **Examination:**Comprehensive documentation of procedures is crucial, including intermittent screenshots for visual evidence.
- **Analysis:**Chain of custody recording may be necessary during this phase.
- **Reporting:**A comprehensive statement outlines tools, data origins, extraction methods, analytical approaches, challenges faced, and resolutions. It must unequivocally demonstrate the unbroken chain of custody for legal validity.

C. PROBLEM STATEMENT

Police departments face the daunting task of managing vast quantities of sensitive digital evidence, underscoring the utmost importance of meticulous packaging, management, and tracking throughout its lifecycle. A robust chain of custody is indispensable to the investigative process, serving as conclusive evidence that digital evidence remains untampered, properly handled, and unaltered. However, a fundamental scientific challenge persists within the current chain of custody framework, as proving the absence of malicious alterations throughout all phases remains unattainable. Numerous challenges confront the chain of custody process, notably encompassing issues of data integrity and the security of documentation. Digital evidence, characterized by its complexity, diffusion, volatility, and susceptibility to alteration, presents manifold indicators signaling potential deficiencies in chain of custody management. These indicators range from threats to the integrity of digital evidence over its lifespan to the monumental task of authenticating massive volumes of data generated by interconnected devices. Addressing this pressing concern necessitates the establishment of a novel framework ensuring the integrity of digital evidence and chain of custody documents. This framework must effectively present data with established integrity, securely store chain of custody records for digital evidence, and offer an auditing mechanism to validate the accuracy of forensic tools and procedures. Leveraging blockchain technology emerges as a promising solution to verify the validity and legality of processes involved in collecting, storing, and transmitting digital evidence, while also providing a consolidated view of all chain of custody interactions. Moreover, blockchain holds potential for evidence verification and management in digital forensics, representing an avenue of exploration in the quest for enhanced integrity and security.

D. MOTIVAION AND CONTRIBUTIONS:

In our groundbreaking project, we introduce the FB-CoC blockchain architecture, designed to tackle challenges in multimedia digital forensic investigations. This architecture ensures complete data provenance, traceability, and assurance throughout the investigative process. By fostering trust in the chain of custody events, it sets a new standard for integrity and reliability in digital evidence handling. It prioritizes privacy protection by encrypting transactional evidence within distributed blocks. Our project reshapes digital forensics, prioritizing security and accountability.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303277 |

II. RELATED STUDY

Digital data analysis for forensic investigations is in high demand due to increased reliance on digital technologies and the rise in cybercrimes. This article introduces an innovative approach using blockchain to assess digital evidence credibility, emphasizing stakeholder involvement in evaluation. It outlines the development of a Global Digital Timeline to document evidence lifecycle activities and proposes a framework integrating Software-Defined Networking and IoT to enhance forensic capabilities. The use of LedgerDB on Alibaba Cloud is suggested for performance enhancement, offering features similar to blockchain. Various methodologies for upholding evidence integrity are explored, including management systems for acquiring digital evidence, blockchain-based integrity verification for video evidence, and securing Electronic Health Records in a cloud environment. The examination of Article 6 of the European Convention on Human Rights highlights the importance of establishing universal rules for evidence governance in digital investigations and addressing challenges specific to digital evidence.

III. PROBLEMS WITH TRADITIONAL JUDICIAL APPROACH

In traditional judicial systems, evidence management relies on manual documentation processes, recording crucial details from collection to court submission. However, this approach faces challenges such as high costs, reliance on legal advocates, and accountability issues leading to delays. Susceptibility to manipulation and lack of transparency further hinder the system. Integrating data across jurisdictions and scalability pose additional challenges. Blockchain technology offers promise in addressing these issues by improving transparency, accountability, and evidence integrity, potentially revolutionizing legal proceedings.

IV. ROLE OF BLOCKCHAIN TECHNOLOGY

Blockchain technology functions as a decentralized system for secure data sharing. It divides data into shared blocks interconnected through unique cryptographic hashes, ensuring integrity and security. There are three primary types of blockchain: public, permissioned/private, and federated/consortium. The process flow involves recording transactions, reaching consensus, linking blocks, and distributing ledger copies. Blockchain significantly enhances the Chain of Custody process in digital forensics by ensuring integrity, traceability, authentication, verifiability, and security of evidence. Integration of blockchain into the Chain of Custody process enables officials to meet these criteria effectively, leveraging blockchain's features of traceability, authenticity, and decentralization to maintain evidence integrity and security.

V. PROPOSED MODEL

At the core of the proposal lies an inventive forensics framework aimed at utilizing blockchain technology to establish a robust Chain of Custody (CoC) while integrating cutting-edge deep learning models for tamper detection. This unified strategy is designed to comprehensively tackle security and forensic needs throughout the entire investigation process.

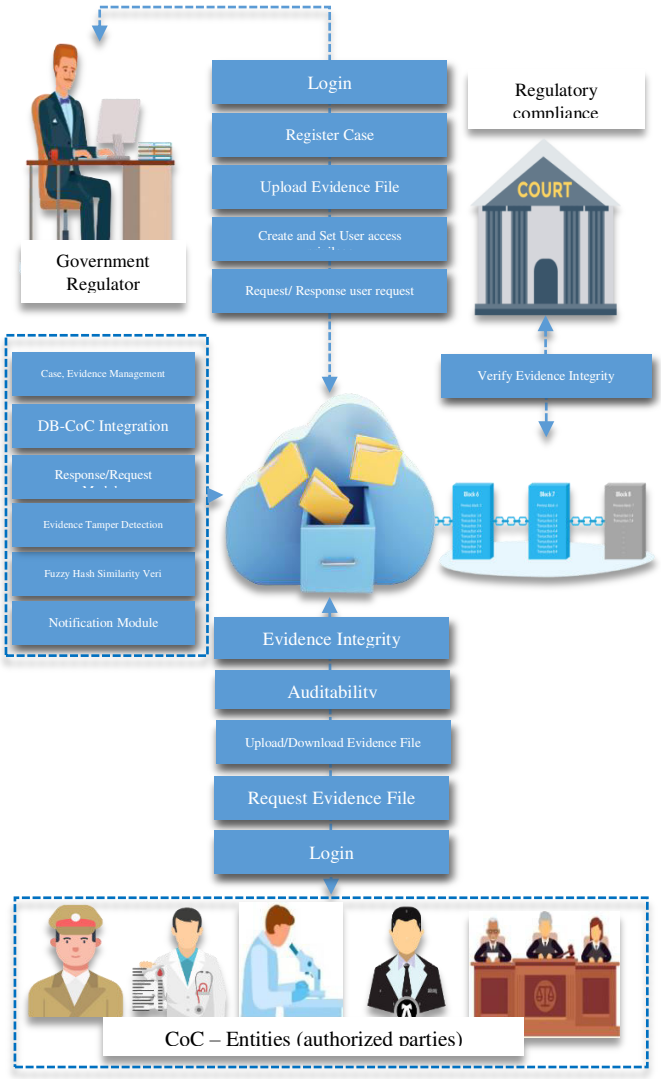
- DB-CoC Architecture: The proposed solution, named DB-CoC, is intricately designed to provide strong information integrity, prevention, and preservation mechanisms. It involves storing evidence (chain of custody) permanently and immutably within a secure, private, permissioned, and encrypted blockchain ledger.
- Blockchain for Chain of Custody: Blockchain technology serves as the cornerstone for ensuring a secure and tamper-proof Chain of Custody. Participants within the investigative ecosystem collaboratively establish a private network to achieve consensus and meticulously document various activities onto the blockchain ledger.
- Advanced Deep Learning Models for Tamper Detection: The proposal advocates for the adoption of diverse deep learning models tailored to detect tampering across various file formats. These models include Image analysis using Convolutional Neural Networks (CNN), Word Document Embeddings employing BERT, Video Frame-level Analysis with Temporal Convolutional Networks (TCN), Audio Spectrogram Analysis utilizing Hidden Markov Models (HMM), and PDF Document Structure Analysis.
- Utilization of Fuzzy Hash Functions: Special emphasis is placed on harnessing fuzzy hash functions, empowering forensic investigators to effectively manage permissible alterations within digital evidence. This involves streamlining forensic procedures to ensure consistency and reliability in evidence handling practices.
- Comprehensive Data Provenance and Traceability: The DB-CoC architecture is committed to providing thorough data provenance and traceability, instilling confidence in the integrity of chain of custody events throughout the entire digital evidence lifecycle, including collection, storage, analysis, and interpretation phases.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303277 |

WORK FLOW:



VI. ALGORITHMS

A. BLOCKCHAIN:

Blockchain technology relies on cryptographic algorithms to establish decentralized, secure ledgers. These algorithms ensure transaction integrity, consensus, and data validation, enhancing trust in digital transactions.

B. DEEP LEARNING:

Deep learning, a subset of machine learning, uses neural networks with multiple layers to extract data representations. Algorithms like CNNs and RNNs excel in tasks like image recognition and predictive analytics, driving advancements in various fields.

C. FUZZY HASH FUNCTIONS:

Fuzzy hashing in computer forensics and cybersecurity identifies data similarities with slight variations. Algorithms like ssdeep and sdhash detect digital artifacts across datasets, aiding in threat detection and evidence tracing for enhanced system security.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303277 |

VII. FUTURE SCOPE

Future endeavors will explore broadening the platform's capabilities to encompass lossless compression and storage optimization. Additionally, novel approaches will be pursued to enhance data ingestion methods and innovate techniques for categorizing the relevance of Multimedia Forensic Digital Evidence (MFDE).

VIII. CONCLUSION

In today's rapidly expanding digital landscape, safeguarding our digital infrastructures against diverse cybersecurity threats presents significant challenges. Digital forensics plays a crucial role in this scenario by conducting systematic investigations and maintaining comprehensive documentation to uncover precisely what transpired within digital networks or computing devices and identify the responsible parties. The primary objective of this project was to develop an FB-CoC model and a platform aimed at securing Multimedia Forensic Digital Evidence (MFDE) to ensure the integrity of stored evidence. The FB-CoC model was specifically designed to assess the effectiveness of fuzzy hashing algorithms within blockchain technology, contrasting them with conventional cryptographic hash algorithms, particularly in image forensics. Results from performance evaluations indicate that fuzzy hash-based blockchains effectively support the chain of custody process by managing realistic workloads with manageable memory overhead for storing the chain and addressing uncertainties related to chain of custody. With the implementation of FB-CoC, investigators are relieved from concerns regarding evidence verification and authenticity during digital investigations.

REFERENCES

1. D. Li, W. Liu, L. Deng, and B. Qin, ``Design of multimedia blockchain privacy protection system based on distributed trusted communication," Trans. Emerg. Telecommun. Technol., vol. 32, no. 2, p. e3938, Feb. 2021.
2. M. Uddin, ``Blockchain medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry," Int. J. Pharmaceutics, vol. 597, Mar. 2021, Art. no. 120235.
3. A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari, and A. E. Rajput, ``MF-ledger: Blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture," IEEE Access, vol. 9, pp. 103637-103650, 2021.
4. M. Li, C. Lal, M. Conti, and D. Hu, ``LEChain: A blockchain-based lawful evidence management scheme for digital forensics," Future Gener. Comput. Syst., vol. 115, pp. 406-420, Feb. 2021.
5. M. R. Kumar and N. Bhalaji, ``Blockchain based chameleon hashing technique for privacy preservation in E-governance system,"Wireless Pers. Commun., vol. 117, no. 2, pp. 1-20, 2020.
6. M. Lusetti, L. Salsi, and A. Dallatana, ``A blockchain based solution for the custody of digital files in forensic medicine," Forensic Sci. Int., Digit. Invest., vol. 35, Dec. 2020, Art. no. 301017.
7. J. Jeong, D. Kim, B. Lee, and Y. Son, ``Design and implementation of a digital evidence management model based on Hyperledger fabric," J. Inf. Process. Syst., vol. 16, no. 4, pp. 760-773, 2020.
8. L. Zarpala and F. Casino, ``A blockchain-based forensic model for financial crime investigation: The embezzlement scenario," 2020, arXiv:2008.07958. [Online]. Available: https://arxiv.org/abs/2008.07958.
9. H. R. Hasan, K. Salah, R. Jayaraman, M. Omar, I. Yaqoob, S. Pesic, T. Taylor, and D. Boscovic, ``A blockchain-based approach for the creation of digital twins," IEEE Access, vol. 8, pp. 34113-34126, 2020.
10. A. H. Lone and R. N. Mir, ``Forensic-chain: Blockchain based digitalnforensics chain of custody with PoC in hyperledger composer," Digit. Invest., vol. 28, pp. 44-55, Jan. 2019.
11. Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, ``Block-DEF: A secure digital evidence framework using blockchain," Inf. Sci., vol. 491, pp. 151-165, Apr. 2019.
12. E. Yunianto, Y. Prayudi, and B. Sugiantoro, ``B-DEC: Digital evidence cabinet based on blockchain for evidence management," Int. J. Comput. Appl., vol. 181, no. 45, pp. 22-29, Mar. 2019.
13. M. Takemiya and B. Vanieiev, ``Sora identity: Secure, digital identity on the blockchain," in Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC), Jul. 2018, pp. 582-587.
14. K. Widatama, Y. Prayudi, and B. Sugiantoro, ``Application of RC4 cryptography method to support XML security on digital chain of custody data storage," Int. J. Cyber-Secur. Digit. Forensics, vol. 7, no. 3, pp. 230-237, 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details