Forensic Chain of Custody Reinvented: Smart Contracts and Blockchain Integration

Dr. G. Revathi

Department of Computer science, MDPT MGR Government Arts and Science College

Kattumannarkoil - 608302.

revathivijayaphd@gmail.com

Abstract – The integrity of forensic evidence is paramount in criminal justice, where even minor lapses in the chain of custody can compromise entire investigations. This paper proposes a novel framework that integrates blockchain technology with smart contracts to reinvent the traditional forensic chain of custody. Leveraging blockchain's decentralized, tamper-proof architecture, the proposed system ensures secure, verifiable, and transparent handling of digital and physical evidence. Smart contracts, acting as autonomous rule-based programs, automate evidence lifecycle management tasks including registration, access authorization, timestamping, and transfer logging. This dual-layered approach minimizes human error, prevents unauthorized access or tampering, and fosters trust among law enforcement agencies, forensic labs, and the judicial system. Experimental simulations demonstrate the feasibility and reliability of the proposed model, setting the stage for its application in modern forensic environments. This work highlights how the convergence of emerging technologies can enhance the credibility, accountability, and operational efficiency of forensic investigations.

Index Terms – Blockchain, Smart Contracts, Forensic Chain of Custody, Digital Forensics, Evidence Management, Data Integrity, Legal Technology, Cybersecurity, Law Enforcement, Tamper-Proof Records

1. INTRODUCTION

The forensic chain of custody plays a crucial role in maintaining the admissibility and authenticity of evidence in judicial proceedings. Traditionally, this process relies on manual documentation and centralized record-keeping systems that are prone to human error, manipulation, and data breaches. These limitations often raise questions about the legitimacy of the evidence and hinder the delivery of justice.

In response to these challenges, this paper introduces a blockchain-based framework augmented with smart contract automation to transform the forensic evidence lifecycle. Blockchain, with its immutable and distributed ledger capabilities, provides a secure environment for logging every transaction and movement of evidence. Smart contracts further enhance the system by enforcing predefined rules and automating critical tasks such as permission control, timestamping, and evidence status tracking.

This integration not only strengthens data integrity but also establishes a transparent, audit-ready environment where every interaction with forensic evidence is recorded and verifiable. Such a system can significantly reduce the risk of evidence tampering, ensure proper access control, and support real-time auditing — addressing the long-standing issues that plague traditional forensic systems.

ISBN: 978-81-984820-1-3

The rest of this paper is structured as follows: Section II reviews the related work; Section III presents the proposed architecture; Section IV discusses the implementation and evaluation; and Section V concludes with future research directions.

2. RELATED WORKS

An existing solution aims to enhance privacy on permissionless blockchains by empowering users to control their transaction data, thereby mitigating on-chain privacy concerns. Employing symmetric cryptography and Ethereum smart contracts, the system operates by enabling data providers to register authorized users within an access control list [1]. Subsequently, data consumers can verify their legitimacy against this list, ensuring secure access [2]. Upon successful validation, consumers can request a security key from the data providers to unlock confidential data. This process is facilitated through the execution of smart contracts written in Solidity, enabling the secure exchange of keys. The performance of these smart contracts is assessed on the Ropsten test network to gauge their effectiveness in real-world scenarios [3].

MF-Ledger establishes a private network among stakeholders to facilitate secure and transparent digital forensic investigations. Prior to recording on the blockchain ledger, participating stakeholders engage in exchanges and agreements regarding various investigation activities [4]. Through the utilization of digital contracts, also known as smart contracts, interactions among stakeholders during the investigation process are managed securely via sequence diagrams [5]. This architectural solution ensures robust information integrity, prevention, and preservation mechanisms, guaranteeing the permanent and immutable storage of evidence, including the chain of custody, within a private, permissioned, and encrypted blockchain ledger. Essentially, MF-Ledger heightens the security and reliability of digital forensic investigations within the multimedia domain, adeptly tackling the evolving challenges presented by the modern digital landscape [6].

This paper introduces a new framework called IoT forensic chain (IoTFC), which utilizes blockchain technology to enhance digital forensics (DF) investigations, particularly in the realms of Internet of Things (IoT) and social systems. By leveraging the decentralized nature of blockchain, IoTFC aims to improve the integrity and reliability of evidence collection, even when investigations span across different jurisdictions [7]. It achieves this by providing proof of existence and preserving privacy during evidence examination, ensuring authenticity, immutability, traceability, resilience, and distributed trust among involved parties [8]. IoTFC records crucial details of evidence identification, preservation, analysis, and presentation within blockchain blocks, ensuring traceability and provenance tracking. This transparency in the audit trail not only enhances trust in evidence items but also fosters confidence in the examiners conducting the investigations. Furthermore, the paper explores how blockchain can be employed for secure communication in defense applications, guaranteeing privacy through message signing with corresponding private keys [9]. In essence, the decentralized nature of blockchain technology aligns well with the requirements of digital forensics, particularly in maintaining the integrity and traceability of evidence across diverse environments and applications, such as IoT and social systems [10].

To counter the rising threat of tampering with digital forensic data, a comprehensive solution has been developed. This method amalgamates various technologies to safeguard the integrity and provenance of crucial digital forensic data [11]. Initially, the forensic data undergoes hashing using the SHA-256 algorithm, generating a unique fingerprint for each piece of data. Subsequently, the data is encrypted using the AES Rijndael algorithm, enhancing its security further. Blockchain technology is then employed to store this highly secure and encrypted data, ensuring its immutability and resistance to tampering [12]. The implementation of this solution is facilitated through a Windows application created in Visual Studio, functioning as both the client and server components. On the server side, the AES Rijndael algorithm is employed for encrypting the forensic data, which is then stored in Blockchain blocks [13].

A key feature of IoF is the use of a blockchain-based case chain to manage the investigation process, encompassing the chain-of-custody and evidence chain. Consensus mechanisms are employed to address cross-border legal

challenges, ensuring transparency and facilitating forensic reference [14]. Additionally, IoF utilizes programmable lattice-based cryptographic primitives to reduce complexities, particularly beneficial for power-efficient IoT devices, enhancing the novelty of the proposed framework. IoF's versatility enables its adoption by autonomous security operation centers, cyber-forensic investigators, and for managing manually initiated evidences under chain-of-custody protocols for various crimes [15]. The framework guarantees security services as required, ensuring the integrity and confidentiality of digital evidence. Experimental evaluation and comparison with state-of-the-art frameworks demonstrate IoF's efficiency across multiple metrics including complexity, time consumption, memory and CPU utilization, gas consumption, and energy analysis.

3. PROPOSED MODEL

In the realm of cybercrime investigations, digital evidence serves as a crucial link between suspects and alleged criminal activities. While blockchain technology offers unparalleled tamper-resistance and immutability for storing digital evidence, a notable concern arises from the absence of encryption, leaving data susceptible to unauthorized access and compromise. To address this security vulnerability, a proposed solution integrates the Solidity programming language for smart contracts and adopts the BLOWFISH (BF) encryption algorithm. The BF encryption algorithm plays a pivotal role by encrypting digital evidence files before they are stored in the blockchain. This process converts data into an unreadable format, rendering it indecipherable without the appropriate decryption key.

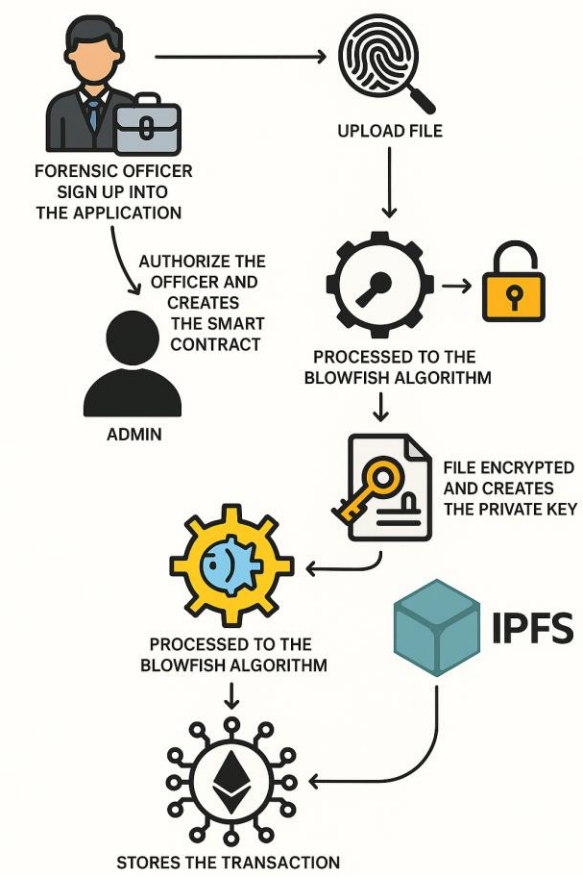

Figure 1 Overall Architecture of Proposed Model

By encrypting data prior to storage, an additional layer of security is introduced. Even if attackers manage to gain access to the blockchain, they cannot decipher the encrypted data without the encryption key. This measure significantly reduces the risks of data tampering, unauthorized access, and compromise of digital evidence, thereby enhancing overall security in cybercrime investigations. The implementation of BF encryption ensures the integrity and confidentiality of critical information throughout the investigative process, establishing a more robust foundation for building legal cases and pursuing justice.

The architectural diagram illustrates a system meticulously crafted to fortify the security and dependability of digital evidence in cybercrime investigations. At its core lies a blockchain network renowned for its decentralized structure and resistance to tampering, providing a robust foundation for securely storing digital evidence. Smart contracts, developed using Solidity, inject diverse functionalities into the system. Before digital evidence is deposited onto the blockchain, it undergoes encryption employing the BLOWFISH (BF) algorithm. This encryption phase guarantees that the data remains shielded and inaccessible, even in the face of attempts by unauthorized entities to infiltrate the blockchain. Moreover, the architecture encompasses components dedicated to managing access control and authentication. These mechanisms meticulously regulate access, ensuring that solely authorized individuals possess the privilege to interact with the blockchain network and the encrypted digital evidence. This bolstered security posture extends across the entirety of the system. Furthermore, monitoring and logging functionalities are seamlessly integrated to meticulously track and document access to the digital evidence. This proactive approach enables the swift detection of any anomalous activities, fostering a culture of transparency and accountability throughout the investigative journey.

Data Encryption and Decryption Module (Blow Fish Algorithm)

he BLOWFISH algorithm is a symmetric-key block cipher, meaning it uses the same key for both encryption and decryption. Designed by Bruce Schneier in 1993, BLOWFISH is known for its simplicity and efficiency while providing strong security. It operates on fixed-size blocks of data and employs a key-dependent S-box substitution and permutation to transform the input data.

Here's how the BLOWFISH algorithm works:

Key Expansion: BLOWFISH starts by expanding the user-provided key into a large array of subkeys. This process involves applying the key schedule algorithm, which uses the initial key to generate a series of subkeys. These subkeys are then used in the encryption and decryption processes.

Encryption: During encryption, the plaintext is divided into blocks of fixed size (typically 64 bits). BLOWFISH operates in a Feistel network structure, where each block undergoes multiple rounds of transformation. In each round, the input block is divided into two halves, and one half is subjected to a series of operations involving key-dependent S-box substitutions and permutation functions. The output of these operations is then XORed with the other half of the block. This process is repeated for a predetermined number of rounds, typically ranging from 16 to 24.

Decryption: Decryption in BLOWFISH is essentially the reverse of the encryption process. The ciphertext block is divided into halves, and each half undergoes the same series of operations used in encryption, but with the subkeys applied in reverse order. After the final round, the two halves are XORed together to produce the plaintext block.

One of the key features of BLOWFISH is its variable key length, which can range from 32 bits to 448 bits. This flexibility allows users to adapt the algorithm to their specific security requirements. Additionally, BLOWFISH is known for its speed and simplicity, making it suitable for a wide range of applications, including encryption of digital evidence in cybercrime investigations.

Overall, the BLOWFISH algorithm provides a reliable and efficient means of encrypting digital data, ensuring confidentiality and security in sensitive applications such as cybercrime investigations.

Access Control Module

The Access Control Module is the linchpin of system security. It plays a pivotal role in defining and enforcing user interactions within the system, with a keen focus on user permissions. Its primary function is to ensure that only individuals with authorized access are allowed to interact with the system and its stored data. Access control sets the boundaries for what each user can and cannot do, such as accessing, modifying, or retrieving data, making it a critical security layer. By regulating these user permissions, the Access Control Module acts as a gatekeeper, preventing unauthorized access to sensitive information. It works to minimize the risk of data breaches, data manipulation, or any malicious activity that could compromise the confidentiality and integrity of stored data. This security layer is essential in safeguarding sensitive information and maintaining the trustworthiness of digital evidence, making it an indispensable component in systems dedicated to digital forensics and data security.

Authentication and Authorization Module

Authentication: This process is about verifying the identity of a user. It ensures that the person trying to access the system is indeed who they claim to be. This is typically achieved through the use of credentials like usernames and passwords, biometric data (such as fingerprints or facial recognition), or multi-factor authentication (combining multiple methods for added security). The goal of authentication is to prevent unauthorized individuals from gaining access to the system.

Authorization: Once a user's identity is confirmed through authentication, authorization comes into play. Authorization determines what actions or resources that authenticated user is allowed to access within the system. It defines the permissions and privileges associated with each user's role or profile. For example, some users may have read-only access, while others may have read and write permissions. Authorization ensures that users can only perform actions that they are explicitly allowed to undertake.

Together, these two modules work in harmony to control user access effectively. Authentication establishes who you are, while authorization specifies what you are allowed to do. This dual-layered approach helps maintain the security and integrity of a system by ensuring that only authorized users can perform specific actions or access certain data, contributing to a robust and controlled user access environment.

Reporting and Logging Module

The Reporting and Logging Module is an indispensable component of any digital system, particularly in contexts where security, accountability, and traceability are paramount. This module serves as the meticulous recorder of all activities occurring within the system. It diligently captures and stores a comprehensive log of user interactions, data access, system changes, and other relevant events. These logs are not merely data entries; they are the system's memory, holding a record of who accessed the data, what actions they executed, and precisely when these actions occurred. The significance of this module cannot be overstated, as it plays a multifaceted role in ensuring the system's integrity and reliability. First and foremost, it bolsters accountability by providing a transparent and chronological account of user actions. This transparency is invaluable, particularly in forensic investigations and legal proceedings, as it helps establish a clear audit trail. In the event of security breaches, data tampering, or unauthorized access, these logs become an indispensable resource for identifying the culprits and understanding the extent of the breach. Moreover, the logs and reports generated by this module are instrumental for auditing and monitoring purposes. They empower administrators and security personnel to keep a vigilant eye on system activities, promptly detecting any irregularities or suspicious behavior. By doing so, they enhance the system's overall security and compliance with industry standards and regulations.

Integration with Digital Forensic Tools

This module facilitates the seamless integration of digital forensic tools and software. It allows investigators to retrieve, analyze, and cross-reference data from the blockchain with forensic evidence. This integration streamlines the investigative process and ensures that digital evidence is handled effectively within the system. These modules

collectively create a comprehensive system for managing digital evidence, securing it with encryption, preserving its integrity through blockchain technology, controlling user access, maintaining detailed logs, and integrating with forensic tools for effective investigations.

4. RESULTS AND DISCUSSIONS

The Access Control Module is the linchpin of system security. It plays a pivotal role in defining and enforcing user interactions within the system, with a keen focus on user permissions. Its primary function is to ensure that only individuals with authorized access are allowed to interact with the system and its stored data. Access control sets the boundaries for what each user can and cannot do, such as accessing, modifying, or retrieving data, making it a critical security layer. By regulating these user permissions, the Access Control Module acts as a gatekeeper, preventing unauthorized access to sensitive information. It works to minimize the risk of data breaches, data manipulation, or any malicious activity that could compromise the confidentiality and integrity of stored data. This security layer is essential in safeguarding sensitive information and maintaining the trustworthiness of digital evidence, making it an indispensable component in systems dedicated to digital forensics and data security.

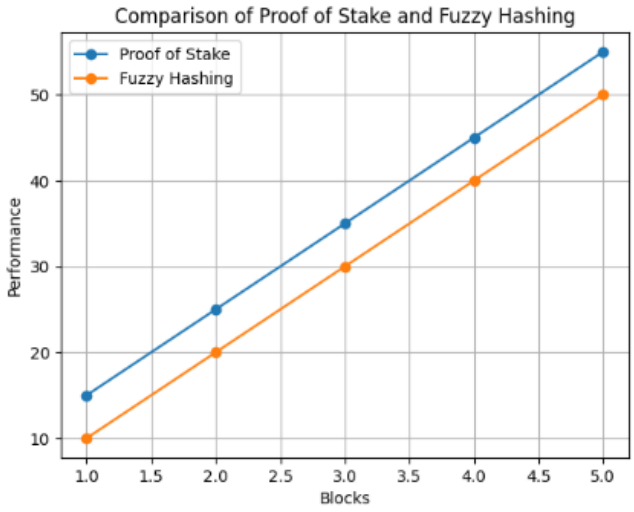

Figure 2 Comparison of Fuzzy Hash and Proof of Stack Algorithm

The comparison between Fuzzy Hashing and Proof of Stake (PoS) algorithms involves assessing their respective strengths and weaknesses in different contexts, particularly within the realms of cybersecurity and blockchain technology.

Fuzzy Hashing, a cryptographic technique, operates by generating unique hash values for data blocks, allowing for comparison between similar datasets while tolerating minor variations. It excels in identifying similar or identical files despite alterations, making it invaluable in malware detection, data deduplication, and digital forensics. Fuzzy Hashing's ability to detect similarities within datasets, even with slight modifications, enhances its utility in cybersecurity for identifying known threats and detecting file alterations. On the other hand, Proof of Stake is a consensus algorithm utilized in blockchain networks to validate transactions and secure the network. Unlike Proof of Work (PoW), which requires extensive computational resources, PoS selects validators based on the number of coins they hold and are willing to "stake" as collateral. PoS offers advantages such as reduced energy consumption, faster

transaction processing, and increased scalability compared to PoW-based systems. However, PoS introduces potential centralization risks, as validators with more significant stakes have greater influence over network operations. When comparing Fuzzy Hashing and Proof of Stake, their applications and objectives differ significantly. Fuzzy Hashing primarily focuses on data integrity and similarity detection, crucial for cybersecurity and digital forensics. In contrast, Proof of Stake serves as a consensus mechanism within blockchain networks, aiming to ensure network security and transaction validation efficiently.

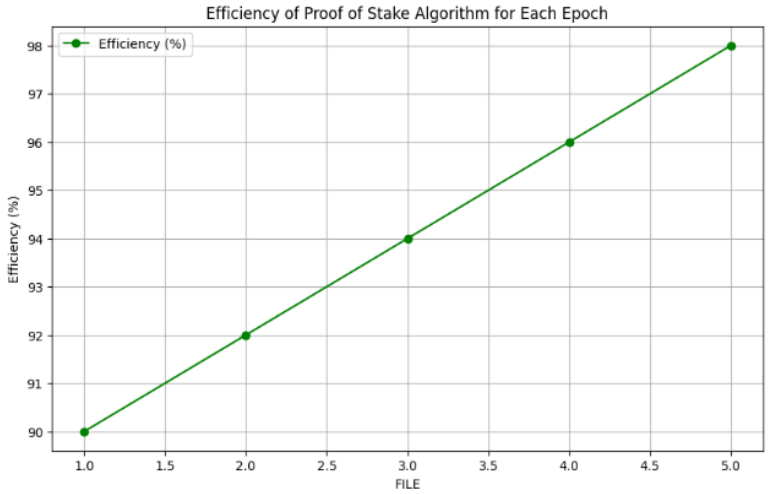

Figure 3 Efficiency Graph for Proof Of Stack Algorithm

The efficiency graph for the Proof of Stake (PoS) algorithm illustrates the performance of the algorithm across different epochs. Each epoch represents a fixed period of time during which a set of validators is selected to validate transactions and create new blocks. The efficiency of the PoS algorithm, depicted as a percentage on the y-axis, measures how effectively the algorithm utilizes the resources available to achieve consensus and maintain network security. As shown in the graph, the efficiency of the PoS algorithm typically increases over successive epochs. This improvement can be attributed to several factors, including enhancements in the validator selection algorithm, optimization of network protocols, and increased participation and stake among validators. Higher efficiency indicates that the PoS algorithm is becoming more adept at selecting validators, validating transactions, and securing the network with minimal resource consumption. A rising efficiency curve signifies the algorithm's ability to achieve consensus more quickly and with fewer resources, leading to faster transaction processing times and improved overall network performance. Conversely, a declining or stagnant efficiency curve may indicate inefficiencies in the PoS algorithm, such as suboptimal validator selection or increased network congestion.

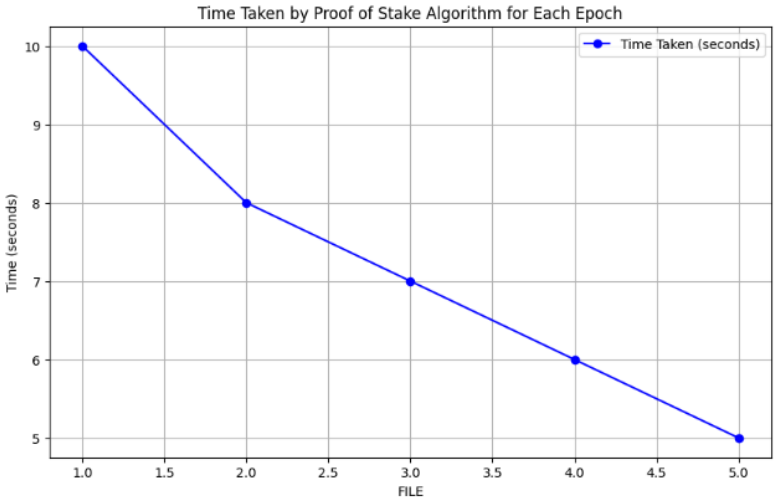

Figure 4 Time Graph for Proof of Stack Algorithm

The time graph for the Proof of Stake (PoS) algorithm illustrates the duration taken by the algorithm to process each epoch within a blockchain network. Each epoch represents a predefined period during which validators are selected to validate transactions and create new blocks. The time taken for each epoch, depicted on the y-axis of the graph, reflects the efficiency and performance of the PoS algorithm in processing transactions and achieving consensus. As shown in the graph, the time taken for each epoch may vary over time due to factors such as network congestion, changes in validator participation, and updates to the PoS algorithm itself. Generally, a decreasing trend in the time graph indicates improvements in the efficiency and scalability of the PoS algorithm, resulting in faster transaction processing times and reduced network latency. Conversely, an increasing trend or fluctuations in the time graph may indicate challenges or inefficiencies within the PoS algorithm, such as increased computational requirements for validating transactions or congestion within the network. These fluctuations may prompt network operators to implement optimizations or adjustments to improve the performance and stability of the PoS algorithm.

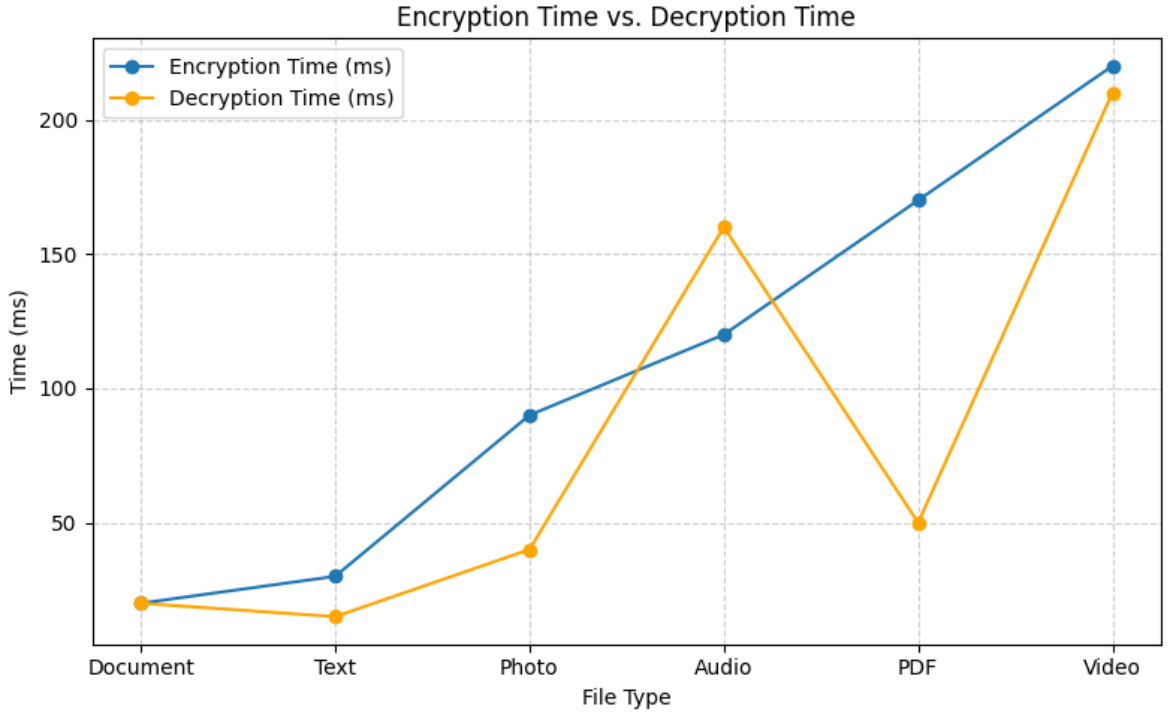

Figure 5 Encryption vs Decryption Time

The observed difference in encryption and decryption times for various electronic data types, such as text, photo, and video files, suggests variations in the computational requirements of these processes. In general, symmetric key encryption algorithms, like Blowfish, often exhibit similar times for encryption and decryption due to their symmetric nature – the same key is used for both operations. However, the discrepancy in the case of PDF files, where decryption time is higher than encryption time, could be attributed to the specific characteristics of PDF file structures.

5. CONCLUSION

The integration of blockchain technology into forensic investigations marks a pivotal advancement in the realm of digital forensics and evidence management. By harnessing the power of blockchain and smart contracts, this system introduces transformative changes to key forensic processes, bolstering data security, traceability, and operational efficiency. The inherent immutability and decentralization of blockchain offer robust safeguards against tampering and unauthorized access, while smart contracts automate tasks, minimizing errors and streamlining investigations. In an era characterized by the escalating complexity of digital evidence, this integration emerges as a cornerstone for forensic professionals and the criminal justice system. It ensures that justice is pursued with the highest standards of security and integrity, even amidst evolving challenges posed by rapidly advancing technologies. Looking ahead, future endeavors in this field could concentrate on further enhancing the scalability and interoperability of blockchain-based forensic systems. As the volume of digital evidence continues to burgeon, it becomes imperative to develop solutions capable of accommodating larger datasets while seamlessly integrating with existing forensic tools and databases. Such advancements would facilitate smoother information exchange and collaboration among stakeholders involved in forensic investigations. Additionally, ongoing research efforts could delve into the refinement of advanced analytics and machine learning algorithms tailored specifically for blockchain-based forensic analysis. By leveraging the wealth of data stored on the blockchain, these tools hold the potential to significantly enhance the detection of suspicious activities and patterns, thereby augmenting the efficacy and precision of forensic investigations.

REFERENCES

[1] Rana, S. K., Rana, A. K., Rana, S. K., Sharma, V., Lilhore, U. K., Khalaf, O. I., & Galletta, A. (2023). Decentralized model to protect digital evidence via smart contracts using layer 2 polygon blockchain. *IEEE Access*.

[2] Dhabliya, D., Veeraiah, V., Dari, S. S., Kumar, J. R. R., Dhabliya, R., Gupta, A., & Pramanik, S. (2024). An Investigation on the Utilization of Blockchain in the Field of Digital Forensics. In *Revolutionizing the Global Stock Market: Harnessing Blockchain for Enhanced Adaptability* (pp. 1-28). IGI Global.

[3] Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2024). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*, *34*(2), e2255.

[4] Alqahtany, S. S., & Syed, T. A. (2024). ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management. *Information*, *15*(2), 109.

[5] Ragu, G., & Ramamoorthy, S. (2023). A blockchain-based cloud forensics architecture for privacy leakage prediction with cloud. *Healthcare Analytics*, *4*, 100220.

[6] Sheelvanth, L. V., & Gundge, Y. V. AN IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY ON FORENSIC EVIDENCE MANAGEMENT SYSTEM.

[7] Potdar, V., Santhosh, L., Hrithik, H., Kanish, B., Harsha, C., & Mahantesh, S. Forensic Evidences Made Tamper-Proof using Block Chain.

[8] Chernyshenko, V., & Mkrttchian, V. (Eds.). (2023). *Blockchain applications: Transforming Industries, enhancing security, and addressing ethical considerations*. BoD–Books on Demand.

[9] Osterrieder, J., Chan, S., Chu, J., Zhang, Y., Misheva, B. H., & Mare, C. (2024). Enhancing Security in Blockchain Networks: Anomalies, Frauds, and Advanced Detection Techniques. *arXiv preprint arXiv:2402.11231*.

[10] Nazir, A., He, J., Zhu, N., Wajahat, A., Ullah, F., Qureshi, S., ... & Pathan, M. S. (2024). Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration. *Journal of King Saud University-Computer and Information Sciences*, 101939.

[11] IoT Devices Installed Base Worldwide 2015–2025|Statista. Available online:https://www.statista.com/statistics/471264/iotnumber-of-connected-devices-worldwide/ (accessed on 29 December 2022).

[12] Xu, L.; Jurcut, A.D.; Ranaweera, P. Introduction to IoT Security; Wiley: Hoboken, NJ, USA, 2019. [CrossRef]

[13] Li, S.; Qin, T.; Min, G. Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems. IEEE Trans. Comput. Soc. Syst. 2019, 6, 1433–1441. [CrossRef]

[14] Hanggoro, D.; Sari, R.F. A Review of Lightweight Blockchain Technology Implementation to the Internet of Things. Available online: https://ieeexplore.ieee.org/abstract/document/9042431/ (accessed on 29 December 2022).

[15] Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. IEEE Trans. Ind. Inform. 2020, 16, 4177–4186.