An Auditable Framework for Evidence Sharing and Management using Smart Lockers and Distributed Technologies: Law Enforcement Use Case.

Belinda I Onyeashie[1], Petra Leimich[2], Sean McKeown[3] and Gordon Russell[4]

[1] Edinburgh Napier University, Edinburgh, Scotland
belinda.onyeashie@napier.ac.uk

Abstract. This paper presents a decentralised framework for sharing and managing evidence that uses smart lockers, blockchain technology, and the InterPlanetary File System (IPFS). The system incorporates Hyperledger Fabric blockchain for immutability and tamper-proof record keeping and employs cryptographic measures to protect the confidentiality of shared and stored evidence. IPFS is employed for secure and efficient storage of digital evidence, while smart lockers provide a solution for managing physical-digital evidence All actions performed on IPFS or smart lockers are recorded on the blockchain, guaranteeing a comprehensive and auditable chain of custody report at the end of an investigation. The goal of this framework is to improve the security, integrity, and accessibility of all digital evidence types, thereby enhancing the efficiency and reliability of investigative processes.

Keywords: Blockchain, Smart Locker, Hyperledger, IPFS, Smart Contracts, Encryption.

1 Introduction

The advent of big data has brought about significant transformations in the landscape of evidence management. The exponential growth in data volume and variety has posed challenges for traditional evidence management systems. The sheer scale and diversity of data sources, including structured and unstructured data, demand innovative approaches to effectively handle and process evidence [1] . Moreover, the integration of diverse evidence data for comprehensive analysis requires scalable and auditable evidence management systems [2]. Traditional centralised systems, with their inherent limitations in scalability and auditability, struggle to meet these demands [3]. Consequently, there is a pressing need to adapt evidence management practices to accommodate the characteristics of big data.

To address these challenges, there is an increasing demand for evidence management systems that can ensure the authenticity, reliability, and accessibility of digital evidence [2]. These systems must be capable of securely storing and managing digital evidence while preserving its integrity and authenticity [4]. Furthermore, they must provide mechanisms to ensure that the privacy and security of the data are upheld [2]. Traditional centralised approaches have demonstrated limitations in guaranteeing data integrity, transparency, and privacy [3]. The process relies on multiple paper forms documents and signature logs that are hard to trace and may be susceptible to errors and issues related to legibility [5]. These challenges necessitate the development of decentralised frameworks that can address these shortcomings and provide robust solutions for evidence storage, sharing and management in the context of the ever-growing volume and complexity of data.

Research on blockchain-based chain of custody for digital evidence management has revealed several gaps. While some studies have examined the use of blockchain for this purpose, most have not adequately addressed the lifecycle of evidence or considered the storage and management requirements of different digital evidence formats.

In this paper, a decentralised framework is proposed for evidence sharing and management using smart lockers and decentralised technologies. Our framework leverages the security and immutability of blockchain to ensure the integrity of evidence, while allowing for efficient and transparent recording and sharing of evidence trails through the use of smart lockers and decentralised technologies. This approach addresses the challenges posed by big data, and evidence management enabling secure and efficient evidence storage, sharing, and management.

The subsequent sections of this paper delve into the current challenges with evidence management process, theoretical foundations, architectural design, implementation details, a brief feasibility highlights and potential future directions of the proposed decentralised evidence sharing and management framework.

1.1 Challenges of Current Evidence Management Processes.

Law enforcement agencies are accumulating massive volumes of digital evidence from body-worn cameras, surveillance systems, social media investigations, and other digital sources. Managing these rapidly expanding big data poses major challenges for evidence integrity and usability [1]. The widespread use of mobile devices such as cell phones and digital cameras has made them prevalent at nearly every arrest and crime scene [6]. As a result, these devices often contain valuable information relevant to criminal activities and necessitate physical seizure and transportation for subsequent analysis [1, 7] . When cyber-physical evidence is seized, it is customarily stored in a secure facility pending analysis and examination [5]. However, this approach and existing digital evidence storage systems have significant limitations some of which are highlighted below:

Centralised Storage Rooms

1. Lack of oversight and reliance on participants to follow protocol leaves room for error or intentional mishandling of evidence [8].
2. Paper logs of access are vulnerable to inaccuracy, loss, or manipulation [5].
3. No system-enforced access restrictions or environmental monitoring [5, 9].

Analog Tracking

1. Paper evidence logs can be forged, omitted, or lost, breaking the chain of custody [5].
2. No immutable record of all interactions with evidence [10].
3. Difficult to coordinate evidence access and transfers between facilities [5, 9].

Limited Security

1. Storage rooms are often secured by normal locks and keys, allowing potential insider threats [5, 9]
2. No transparent systemised tracking of who accessed evidence or when [10].
3. Evidence can be tampered with or degraded without detection [7].

Law enforcement must prioritise the integrity, security, and privacy of evidence [7]. A robust architecture is required to effectively harness big data in policing and to guarantee the reliability of evidence. A shift towards decentralised evidence management could improve security, accessibility, and management at the big data scale [1]. Potential solutions include technologies such as blockchain, distributed storage, advanced access controls, and standardised metadata for efficient digital evidence management [11] (Wang et al., 2021).

2 Relevant Technologies

This section will discuss the relevant technologies that are essential to the proposed framework for evidence sharing and management. These technologies provide the foundation for our decentralised approach, enabling a complete lifecycle of digital evidence management. The key features and suitability of these technologies will be explored and their relevance to the problem statement discussed in Section 1.

Existing approaches to digital evidence storage and management, such as centralised databases, have evolved to address the complexities of handling large amounts of evidence. However, these traditional methods suffer from potential single points of failure from centralised data centre, vulnerability to unauthorised access, and data tampering risks [10]. While blockchain has been proposed as a solution to monitor evidence trails, current approaches do not fully encompass the entire lifecycle of evidence [12]. Most approaches [13-16] only cater to specific types of evidence and do not consider the management of physical-digital evidence seized during investigation. This oversight can lead to challenges in tracing potential tampering or data loss during evidence acquisition.

An evidence management system is incomplete if the storage architecture for evidence is not clearly defined. The system should cover the entire lifecycle of evidence, which includes acquisition of data from source, preservation, analysis, storage, and presentation in court [5]. However, in the current research on this topic, there is inconsistency in the methods employed for storing digital evidence, and often, the specific non-blockchain evidence storage architecture utilised is not explicitly disclosed. Additionally, managing the chain of custody and ensuring data integrity in a dynamic and collaborative investigative environment remains challenging.

The remainder of this section will discuss technologies which each address an element required to render a functioning cyber-physical evidence management system:

i) Blockchain, providing an auditable ledger of user access and data manipulation.
ii) Storage technologies for large scale evidence storage and sharing; and
iii) Encryption principles which facilitate appropriate user access and control.

2.1 Blockchain and Its Feasibility for Evidence Storage

Blockchain technology has emerged as a potential solution to complement big data by offering improved auditability, enhanced data integrity, real-time data analytics capabilities, and improved overall quality of big data [17]. However, storing sensitive data directly on the blockchain is not a recommended practice in the context of digital evidence management [12]. While blockchain technology offers several advantages such as immutability, decentralisation, and transparency, it is not designed to handle large volumes of sensitive data efficiently and securely.

Blockchain networks consist of multiple nodes that replicate and store the entire transaction history, including all data stored on the blockchain. As the volume of data increases, the storage requirements for each node become significantly larger, which can hinder the performance and scalability of the blockchain network [18]. Storing sensitive data directly on the blockchain would exacerbate this scalability challenge, making it impractical for managing large amounts of digital evidence.

Another concern is data privacy and confidentiality [2]. Blockchain networks are inherently transparent, meaning that all transactions and data stored on the blockchain are visible to all participants. While the data itself is secured through cryptographic algorithms, the metadata associated with transactions, including timestamps and transaction hashes, can still reveal sensitive information. Storing sensitive data on the blockchain would compromise the privacy and confidentiality of that data [2], which is a critical consideration when dealing with digital evidence. Instead, the blockchain is primarily used to record the chain of custody, which is a document that records the sequential trail of evidence as it passes through different departments and participants at each stage of an investigation [5]. The chain of custody records data on the method, time, place, and participant who handled the data during its acquisition, processing, storage, and eventual use in investigations. This ensures that the information presented has not been tampered with and is genuine before it is admitted into evidence, thus ensuring the integrity and traceability of digital evidence [2, 12]. However, with the traditional approach of manually handling chain of custody on paper, the chain of custody may be susceptible to human error or erasure, making it difficult to evidence integrity [12]. The blockchain, with its decentralised and immutable features, may be the ideal technological framework for this purpose as a log of all evidence activity can be stored and generated from the blockchain to prove or disprove a case [2, 12]. Consequently, while the blockchain serves as a medium to log the chain of custody, the actual sensitive evidence data can be stored on a scalable and efficient system designed for managing and storing diverse cyber-physical evidence data.

2.2 Evidence Storage Architectures

Digital evidence storage architecture consists of technology, software, and methods for storing and managing digital evidence. The storage of digital evidence needs to be designed with the investigators' time and ability to work without being hindered by their location in mind [9]. Various architectures for storing digital evidence have been developed and are classified as either centralised, decentralised, or hybrid.

In a centralised storage system, all digital evidence is held in a single location, which is often a server or collection of servers [10]. This method is easy to handle because all the evidence is stored in one area and can be accessed by authorised staff from any location. However, because all evidence is maintained in a single area, centralised storage systems may be susceptible to security breaches [12].

Evidence stored in a centralised location can be fraught with challenges including security breaches, modification and issue in the reliance on manual evidence intake processes, which can be time-consuming and prone to errors or legibility issues [9]. However, centralised evidence storage cannot be completely eliminated as evidence such as mobile phones, laptops etc when seized may require a temporary storage location before analyses. Additionally, automating, and digitising evidence access can therefore bolster the chain of custody, such as with smart lockers with automatically evidence access to the items within.

Smart lockers in a centralised location can help to mitigate these issues by providing automated documentation which can protects evidence integrity. Bowes [19] highlights the adoption of smart lockers by law enforcement agencies aiming to modernise their evidence management practices. These smart lockers create a digital record that includes when evidence is deposited and by whom, as well as when it is retrieved by an evidence custodian [19]. This reduces the risk in short-term evidence management and complies with digital forensic procedures for evidence management before it is uploaded to the distributed storage system after analysis.

Distributed file storage systems have gained popularity for data storage and management [20]. The distributed peer-to-peer function of these systems provides a useful alternative to centralised file storage, addressing issues related to data sharing and availability in the event of system failure. Figure 1 shows the characterisation of storage types, including popular software defined storage systems such as Ceph, GlusterFS, IPFS, and HDFS. Le, et al. [21] summarised the features and drawbacks of these file systems and evaluated IPFS in terms of performance and security. Building on positive research findings from evaluations of IPFS performance and its interoperability with blockchain to safely scale and manage big data, this paper proposes utilising IPFS for this framework.

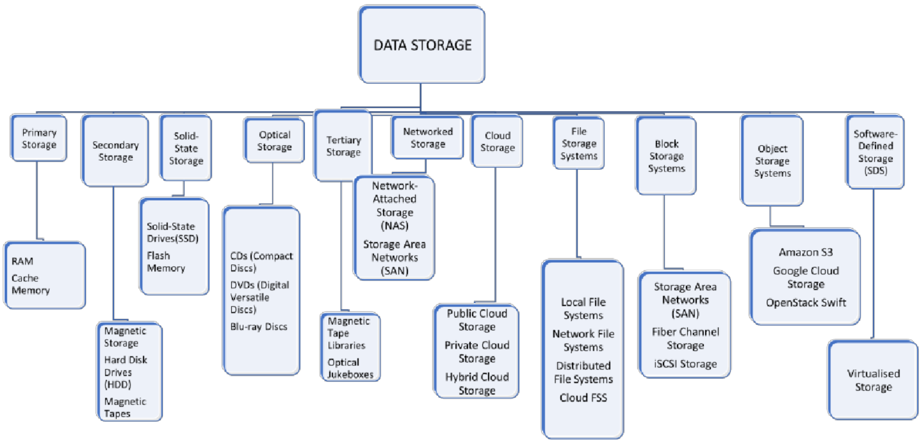

Figure 1: Characterisation of storage types

2.3 IPFS

IPFS is a distributed file system that provides a decentralised approach to storing and sharing data. It ensures data integrity through a content-addressable file system, where files are identified by their content rather than their location [21, 22]. Each file is assigned a unique cryptographic hash, which serves as its identifier.

In traditional centralised storage systems, the integrity of data can be compromised if a single point of failure occurs. In contrast, IPFS is designed to facilitate efficient and decentralised data storage, with files distributed across multiple nodes in the network [22]. The content-addressable nature of IPFS enables seamless data sharing and collaboration. Additionally, IPFS is designed to handle large-scale data storage and retrieval [22], with its distributed architecture allowing for the addition of new nodes to accommodate increasing volumes of digital evidence. This scalability is critical in big data management, where the volume and variety of digital evidence sources can be substantial.

2.4 Encryption Methods (Evidence Security and Access Control)

The use of blockchain and distributed storage systems alone is not sufficient for managing sensitive confidential data as evidence. These systems must be incorporated into a comprehensive evidence management system that encompasses the entire lifecycle of evidence. The storage and sharing of digital evidence in investigations pose challenges related to the need for encryption and secure sharing methods among multiple participants [15] . These challenges as outline above include concerns about the authenticity, integrity, privacy, and security of the evidence, as well as difficulties associated with digital forensic processes [2]. Encryption algorithms are essential for ensuring security and confidentiality of evidence during data sharing in investigations., investigators can ensure access is limited to authorised participants by encrypting data. This is important for digital evidence as it can be easily copied or tampered with if not secured.

There are several encryption algorithms that can be used for file sharing. Symmetric and asymmetric encryption algorithms are fundamental types of encryptions used to secure data [23]. Symmetric encryption uses the same key for encryption and decryption. Examples include AES, DES, and TripleDES. Asymmetric encryption uses a pair of keys: one for encryption and one for decryption. Examples include RSA, DSA, CP-ABE and ECC. The public key encrypts data, while the private key decrypts it [24]. Asymmetric encryption is often used for secure communication over the internet, such as in SSL/TLS protocols [23].

RSA: RSA, introduced in 1977, is used for data encryption and digital signatures. A public key is generated by multiplying two large prime numbers and choosing an integer coprime to the totient of the product [24]. RSA's security relies on the difficulty of factoring the product of two large prime numbers [25]. Since its introduction, no major weaknesses have been successfully exploited in the algorithm.

CP-ABE Method: CP-ABE specifically refers to Ciphertext-Policy Attribute-Based Encryption. In CP-ABE, the access control policy is defined over attributes associated with the users and the encrypted data [26]. The encryption scheme allows fine grained access control, where the decryption of the encrypted data is only possible for users who possess attributes that match the specified policy [27]. CPABE provides flexibility in defining access control policies, allowing complex logical expressions to be used in determining access rights. This makes it suitable for scenarios (such as this use case) where access control requirements are based on multiple attributes and complex conditions. It enables secure and efficient sharing of encrypted data while maintaining control over who can access the decrypted information. The access control strategy in CP-ABE is encrypted into the ciphertext. This feature makes it suitable for data sharing use cases.

3 System Overview

The process of managing digital evidence comes with considerable challenges, primarily legal preservation of data and facilitating investigative access. However, a system that integrates blockchain smart lockers with the InterPlanetary File System (IPFS) presents substantial advantages, particularly for maintaining the chain of custody and fostering collaboration [22]. When authorities seize physical devices such as laptops or phones, a blockchain ledger immutably records their storage in tamper-resistant smart lockers. This procedure cryptographically validates the chains of custody and securely stores the evidence in controlled environments.

Once authorised, investigators extract digital evidence from source devices and securely save it on IPFS. In the process, smart contracts record these actions on the blockchain, thereby promoting accountability. Smart contracts [11] function as the rule's engine, enabling tamper-resistant automation of evidence sharing and auditing.

Furthermore, the decentralised nature of the IPFS network eliminates central points of failure and allows authorised participants to access and analyse evidence concurrently and in a permissioned manner [22]. IPFS integrates with blockchain ecosystems to connect off-chain evidence files with on-chain evidence metadata. This approach facilitates efficient collaboration across agencies while retaining control over the data [22]. Robust access logs and encryption mechanisms ensure enhanced security. The combined architecture maintains immutable custody records, negates insider threats, and enables large-scale controlled evidence sharing and storage. This integration simplifies digital evidence management while upholding evidentiary standards.

3.1 System Requirements

Based on the gaps identified in literature and in practice, the system will prioritise the secure management and preservation of digital evidence throughout its entire lifecycle. The system aims to manage all kinds of digital evidence including cyber-physical evidence. This includes implementing measures to protect against unauthorised access, tampering, or deletion, and employing encryption techniques to safeguard confidentiality. Access controls will ensure that only authorised individuals can view or share evidence.

The proposed system aims to achieve secure storage of all evidence types, allowing for seamless sharing among participants regardless of their location. Relevant metadata, such as timestamps, file properties, geolocation data, or device information, will be recorded and organised on a permissioned blockchain. A permissioned blockchain as the name implies, is invitation-only [18]. This is to ensure the integrity of the network and that only trusted participants may have access to the system data.

The system will support collaboration among participants involved in an investigation, providing features for secure communication, sharing of evidence, and collaborative analysis. Case management functionalities will enable investigators to organise and track the progress of assigned cases, assign tasks, and generate reports.

Maintaining a reliable chain of custody is crucial in digital investigations. The system will track the movement of digital evidence from the time of collection to its use in investigation, automatically logging actions taken on the system. The system will support the generation of a comprehensive, non-repudiated, and auditable chain of custody log, allowing participants to extract relevant information and present it in a manner that is admissible in court.

3.2 System Design and Case Study

The proposed decentralised evidence sharing, and management framework integrates smart lockers, permissioned blockchain technology, and the InterPlanetary File System (IPFS) to address the challenges of traditional centralised approaches. Smart lockers provide secure storage for physical devices containing digital evidence, while a permissioned Hyperledger blockchain establishes a trust framework and maintains an immutable ledger of transactions. IPFS enables decentralised and efficient storage of evidence files, and smart contracts automate evidence management processes.

The system includes participants such as law enforcement agencies, investigators, courts, and lawyers, with an investigation administrator or controller maintaining evidence and granting access privileges. The blockchain maintains an access control list for both the smart locker and IPFS, and there is a requirement for multiple physical partipants to cross verify physical interactions with the smart locker. The permissioned blockchain provides a secure and transparent way to manage access to the smart locker and IPFS, with different access levels granted to participating nodes.

The proposed framework is divided into four main phases: Participant Registration and Authentication, Evidence encryption and storage, Evidence retrieval, Chain of Custody report generation.

Participant Registration and Authentication Phase: The Investigator Administrator (IA) serves as the system controller; they are usually responsible for initialising and registering the participants. The IA is usually an entity that has been confirmed to have no conflicts of interest with the investigation.

This phase involves the IA generating a public key and primary secret key using the CP-ABE algorithm. Each participant is assigned a private key that corresponds to their specific attribute set. These attributes define the access policies or permissions granted to each participant. The IA receives the participant's public key and encrypts their private key using RSA encryption, then securely distributes the encrypted private keys to their respective participants.

The proposed encryption method ensures the privacy and security of digital evidence before it is uploaded to the distributed storage system. First, the investigator administrator encrypts the digital evidence then, the encrypted digital evidence is uploaded or stored to either the distributed storage system or the smart locker depending on the evidence type. The encrypted digital evidence (hash value) is obtained and stored to the blockchain.

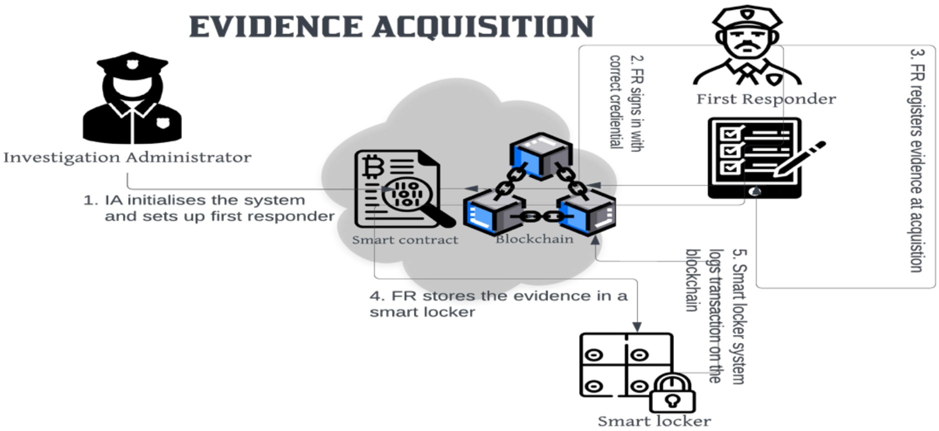
EVIDENCE ACQUISITION
Investigation Administrator
1. IA initialises the system and sets up first responder
Smart contract
Blockchain
First Responder
2. FR signs in with correct credential
3. FR registers evidence at acquistion
4. FR stores the evidence in a smart locker
5. Smart locker system logs transaction on the blockchain
Smart locker

Figure 2: Evidence acquisition and storage to blockchain based-smart locker.

Evidence Encryption and Storage Phase: The evidence encryption and storage phase are initialised in two ways. If the evidence acquired is unstructured that is, in its raw unprocessed form e.g., laptop, mobile phones etc. containing evidence, then it will need to first be registered on the blockchain, then stored in the smart locker for the appropriate department/ participant to retrieve for analysis. Otherwise, if the evidence is already digitised, then it can be encrypted and stored directly to the distributed storage system. The smart locker is blockchain based and is part of the main system. Every action taken on the smart locker is automatically recorded on the blockchain.

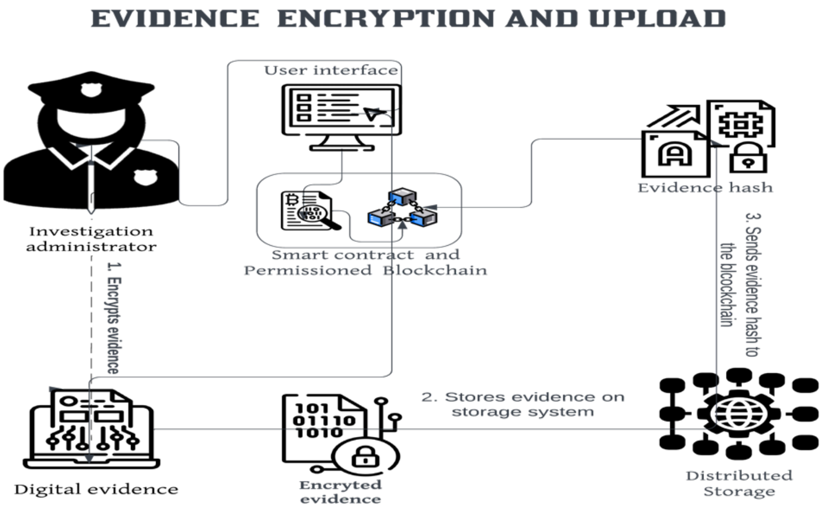
EVIDENCE ENCRYPTION AND UPLOAD
User interface
Investigation administrator
Smart contract and Permissioned Blockchain
Evidence hash
3. Sends evidence hash to the blocckchain
1. Encrypts evidence
Digital evidence
Encryted evidence
2. Stores evidence on storage system
Distributed Storage

Figure 3: Evidence encryption and upload

Evidence Retrieval Phase: An evidence requester such as digital investigator, etc, can obtain the encrypted evidence hash value, evidence data and other data like chain of custody log only when they meet certain conditions. When a participant receives the encrypted digital evidence from the IA, obtained from IPFS using its content identifier (CID). They then use their CP-ABE private key to decrypt the evidence, and if their attribute set satisfies the predefined access criteria, they can successfully access the evidence's contents.

Participants private keys will be sent through a secure off-blockchain communication channel to improve scalability and avoid system overhead. A participant does not need to receive a new encrypted private key every time they request evidence, as their private key is associated with their attribute set and can be used to decrypt any ciphertext with an access policy satisfied by their attributes. Once the participant has received and decrypted their encrypted private key from the IA using their RSA private key, they can use their CP-ABE private key to decrypt any authorised encrypted evidence. If their attribute set changes or their old private key is compromised, the IA will generate a new CP-ABE private key for the participant, encrypt it using the participant’s public key, and securely transmit it to them.

Chain of Custody Report Generation: The log of every action taken on the smart locker and distributed storage recorded on the blockchain, creating an immutable and transparent audit trail of system activity. When requested, maybe by the court, the IA can generate comprehensive reports of the evidence trail throughout the investigation. The court can also be granted access by the IA to verify the chain of custody.

4 Conclusions

The Decentralised Evidence Sharing and Management Framework presented in this paper offers a secure and comprehensive solution for cyber-physical evidence in investigative processes. The integration of these components (Permissioned blockchain, IPFS and smart locker) ensures data immutability, secure storage of evidence and enables the recording of every action taken during an investigation, establishing a transparent and accurate chain of custody report. Additionally, cryptographic techniques protect sensitive information and enforce access controls to ensure that only authorised participants can access and share evidence.

Implementing emerging technologies like blockchain and IPFS necessitates resolving concerns regarding their viability in the real world. As law enforcement agencies seek to improve their evidence management systems, it is logical to assess the feasibility of transition efforts before proceeding. Future works will include an implementation and a detailed feasibility assessment of the proposed framework.

The framework addresses challenges in evidence management, including storage, sharing, tampering risks, and unauthorised access. The successful deployment of this system promises a robust foundation for efficient and secure evidence management and improve the reliability of digital evidence in our progressively digital era.

References

[1] T. D'Anna *et al.*, "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," (2023).

[2] M. Li, C. Lal, M. Conti, and D. Hu, "LEChain: A blockchain-based lawful evidence management scheme for digital forensics," *Future Generation Computer Systems,* vol. 115, pp. 406-420, (2021).

[3] S. Soltani and S. A. H. Seno, "A survey on digital evidence collection and analysis,," *7th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran,* (2017).

[4] A. A. Khan, A. A. Shaikh, and A. A. Laghari, "IoT with multimedia investigation: A secure process of digital forensics chain-of-custody using blockchain hyperledger sawtooth," *Arabian Journal for Science and Engineering,* pp. 1-16, (2022).

[5] U. Sisodia, "Chain of Custody: Scaling the Investigation to the Event," in *Crime Scene Management within Forensic Science: Forensic Techniques for Criminal Investigations*: Springer, (2022).

[6] M. Okmi, L. Y. Por, T. F. Ang, W. Al-Hussein, and C. S. Ku, "A systematic review of mobile phone data in crime applications: a coherent taxonomy based on data types and analysis perspectives, challenges, and future research directions", (2023).

[7] A. F. Moussa, "Electronic evidence and its authenticity in forensic evidence," *Egyptian Journal of Forensic Sciences,* (2021).

[8] A. Singh, R. A. Ikuesan, and H. Venter, "Secure storage model for digital forensic readiness," *IEEE Access,* vol. 10, (2022).

[9] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "The Framework to Support the Digital Evidence Handling," *Journal of Cases on Information Technology,* vol. 22, 2020.

[10] S. Rao, S. Fernandes, S. Raorane, and S. Syed, "A Novel Approach for Digital Evidence Management Using Blockchain," (2020).

[11] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* vol. 49, no. 11, pp. 2266-2277, (2019).

[12] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," *Information Sciences,* vol. 491, pp. 151-165, (2019).

[13] R. Biswas and S. Biswas, "Blockchain Based Digital Forensics: A Fundamental Perspective," in *Artificial Intelligence and Blockchain in Digital Forensics*: River Publishers, (2023).

[14] 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, (2021).

[15] H. Chougule, S. Dhadiwal, M. Lokhande, R. Naikade, and R. Patil, "Digital Evidence Management System for Cybercrime Investigation using Proxy Re-Encryption and Blockchain," *Procedia Computer Science,* vol. 215, pp. 71-77, (2022).

[16] M. Chopade, S. Khan, U. Shaikh, and R. Pawar, "Digital forensics: Maintaining chain of custody using blockchain," (2019).

[17] N. Deepa *et al.*, "A survey on blockchain for big data: approaches, opportunities, and future directions.," *Future Generation Computer Systems.,* (2022).

[18] R. Ramadoss, "Blockchain technology: An overview," *IEEE Potentials,* vol. 41, no. 6, pp. 6-12, (2022).

[19] P. Bowes. "Irrefutable evidence: Modern technology transforms short-term storage." https://www.pitneybowes.com/us/blog/how-smart-lockers-improve-evidence-management.html accessed 05/07/2023, (2023).

[20] A. M. Faruq, S. M. Andri, and P. Yudi, "Clustering storage method for digital evidence storage using software defined storage," (2020).

[21] V. Le, R. Moazeni, and M. Moh, "Improving Security and Performance of Distributed IPFS-Based Web Applications with Blockchain," Springer, pp. 114-127, (2021).

[22] S. Jamulkar, P. Chandrakar, R. Ali, A. Agrawal, and K. Tiwari, "Evidence management system using blockchain and distributed file system (ipfs),"Springer, pp. 337-359, (2022).

[23] M. E. Smid, "Development of the advanced encryption standard.," *Journal of Research of the National Institute of Standards and Technology, 126.,* (2021).

[24] S. Nisha and M. Farik, "Rsa public key cryptography algorithm–a review.," *International journal of scientific & technology research, 6(7),* (2017).

[25] A. Hamza and B. Kumar, "A review paper on DES, AES, RSA encryption standards.," *In 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART). IEEE.,* (2020).

[26] S. Zhang, L. Li, L. Chang, T. Gu, and H. Liu, "A ciphertext-policy attribute-based encryption based on Multi-valued decision diagram.,. *Springer International Publishing.,* (2018).

[27] K. Sethi, A. Pradhan, and P. Bera, "Practical traceable multi-authority CP-ABE with outsourcing decryption and access policy updation.," *Journal of Information Security and applications, 51, p.102435.,* (2020).