

**BLOCKCHAIN BASED CRIMINAL INFORMATION
MANAGEMENT SYSTEM IN SRI LANKA: SECURE
FILE MANAGEMENT SYSTEM IN DECENTRALIZED
NETWORK**

M.N Haseef Ahmed

IT20157814

BSc (Hons) in Information Technology

Specializing in Cyber Security

Department of Computer System Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

September 2023

BLOCKCHAIN BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA: SECURE FILE MANAGEMENT SYSTEM IN DECENTRALIZED NETWORK

M.N Haseef Ahmed

IT20157814

Dissertation submitted in partial fulfillment of the requirements for the Bachelor of
Science in Information Technology Specializing in Cyber Security

Department of Computer System Engineering

Sri Lanka Institute of Information Technology, Sri Lanka

September 2023

DECLARATION

I declare that this is our own work, and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Name	Student ID	Signature
M.N Haseef Ahmed	IT20157814	

The above candidate is carrying out research for the undergraduate Dissertation under my supervision.

Signature of the supervisor

Date

.....

.....

(Mr. Kanishka Yapa)

Signature of the co-supervisor

Date

.....

.....

(Ms. Dinithi Pandithage)

ACKNOWLEDGEMENT

I would like to extend my heartfelt gratitude to the numerous individuals whose contributions have been instrumental in the development of this project. First and foremost, I would like to express my sincere appreciation to my esteemed Supervisor, **Mr. Kanishka Yapa**. His unwavering guidance, expert insights, and continuous support have been invaluable throughout the entire process of this research. And want to extend my thanks to my Co-Supervisor, **Ms. Dinithi Pandithage**. Her expertise and thoughtful input have significantly enriched the quality of this project. Her guidance has been instrumental in shaping the direction of this research endeavor. Moreover, I am deeply grateful to the dedicated members of the Research Team for their significant contributions and support. Their collective efforts and valuable suggestions have played a pivotal role in refining the concepts and methodologies. And sincerely thankful to all those who have offered their expertise, time, and encouragement. Your contributions have been essential to the successful development of this project.

ABSTRACT

Criminal information management systems collect and store massive amounts of data in police stations. Such as personal identification information, criminal records, forensic evidence and many more. It is a responsible to consider security of this information. Because of that plan to implement a decentralized network. The idea behind this decentralized (blockchain) technology is “**Satoshi Nakamoto**”. When implemented a blockchain based criminal management system, it can store sensitive information more securely in a decentralized network. To ensure confidentiality, integrity, and availability of information. Therefore, implement a **secure file management system in a decentralized network** for (CIMS). Moreover, Implementation of IPFS technology ensures a confidentiality, integrity, and availability of the information. And improve the speed, reliability, and security of the system.

Keywords: Blockchain, Criminal Records, Decentralized Network, IPFS, Secure File Management.

TABLE OF CONTENTS

DECLARATION	i
ACKNOWLEDGEMENT	ii
ABSTRACT.....	iii
TABLE OF CONTENTS.....	iv
LIST OF TABLES.....	v
LIST OF FIGURES	vi
LIST OF ABBREVIATIONS.....	vi
1. INTRODUCTION	1
1.1 Background Literature.....	1
Implementing secure file management system	2
1.2 Research Gap.....	8
2. RESEARCH PROBLEM	10
3. RESEARCH OBJECTIVE	12
3.1 Main Objective.....	12
3.2 Specific Objectives.....	13
3.2.1 Secure File Management System in a Decentralized Network.....	13
3.2.2 Advantages of Blockchain-based Criminal Information Management Systems	13
3.2.3 Implementing Cryptography for Enhanced Security	14
3.2.4 Symmetric Encryption for Permanent File Storage	15
3.2.5 Secure File Sharing with Asymmetric Encryption	15
4. METHODOLOGY	16
4.1 File Upload and Token Generation Process in the Criminal Management System ..	16
4.2 Secure Storage of Criminal Information and Evidence	18
4.3 Secure File Sharing Management System.....	20

4.4	Development of a Criminal Information Management System	21
4.5	Implementing a Secure File Management System	23
4.6	Integrating a Secure File Management System with Blockchain	25
4.7	Implementing Cryptography for Data Security	27
4.7.1	Cryptographic File Storage in IPFS	27
4.7.2	Cryptographic File Sharing via IPFS	28
4.8	Technology Used in Project	29
4.9	Software Specification	30
5.	TESTING AND IMPLEMENTATION RESULTS AND DISCUSSION.....	33
5.1	Secure File Sharing in Decentralized Network	33
5.2	Secure File Management System in Decentralized Network.....	36
5.2.1	Upload Files to IPFS	37
5.2.2	Download File From IPFS	38
5.2.3	Integrity Check of The File.....	39
5.2.4	Send Token to Blockchain	40
6.	COMMERCIALIZATION	41
7.	CONCLUSION	42
8.	REFERENCES	43

LIST OF TABLES

<i>Table 1: Research Gap</i>	9
<i>Table 2: Technologies</i>	29

LIST OF FIGURES

<i>Figure 1: Secure File Management System</i>	<i>16</i>
<i>Figure 2: Secure File Management System to Store Files</i>	<i>18</i>
<i>Figure 3: Secure File Management System to Share Files.....</i>	<i>20</i>
<i>Figure 4: Asymmetric Encryption (Select File)</i>	<i>33</i>
<i>Figure 5: Asymmetric Encryption (Select Public Key).....</i>	<i>34</i>
<i>Figure 6: Encrypted Successfully</i>	<i>34</i>
<i>Figure 7: Asymmetric Decryption</i>	<i>35</i>
<i>Figure 8: Successfully file Decrypted.</i>	<i>35</i>
<i>Figure 9: UI of Secure File Management</i>	<i>36</i>
<i>Figure 10: Upload Files to IPFS</i>	<i>37</i>
<i>Figure 11: Download file from IPFS.....</i>	<i>38</i>
<i>Figure 12:Uploaded File Hash.....</i>	<i>39</i>
<i>Figure 13:Downloaded File Hash.</i>	<i>39</i>
<i>Figure 14: Send token to Blockchain.....</i>	<i>40</i>
<i>Figure 15: Store CID value in Blockchain</i>	<i>40</i>

LIST OF ABBREVIATIONS

Abbreviation	Description
1. IPFS	InterPlanetary File System
2. CIMS	Criminal Information Management System
3. SQL	Structured Query Language
4. DoSS	Distributed Denial of Service
5. DHT	Distributed Hash Table
6. PII	Personal Identification Information
7. FIR	First Incident Report
8. API	Application Programing Interface

1. INTRODUCTION

1.1 Background Literature

Due to the alarming rise in criminal activities, there is an urgent need to establish a more efficient and secure system for managing criminal information. A significant drawback of the traditional approach to criminal data management lies in its reliance on paper-based records, which are susceptible to loss or theft. Furthermore, these records are typically stored in a centralized database, which poses several critical issues. This centralized system lacks robust security measures, transparency, and fails to adequately preserve data integrity and consistency over time. Consequently, unauthorized data modifications and data breaches have occurred, compromising the confidentiality and privacy of sensitive information [1].

To address the shortcomings of current systems and ensure secure and transparent solutions for the storage and sharing of criminal records, blockchain technology presents a viable alternative. Blockchain is a decentralized and immutable ledger that records transactions in a transparent and highly secure manner. Each block in the blockchain contains a hash of the preceding block, making it virtually impossible to tamper with the stored data. The ledger is distributed across a network of nodes, eliminating the existence of a single point of failure, and providing robust protection against malicious activities. In a blockchain-based criminal information management system, individual criminal records can be stored as separate blocks on the chain, accompanied by metadata such as date, time, location, and type of crime. Access to this information is restricted to authorized personnel, including police officers and law enforcement agencies, secured through stringent authentication methods [2].

The adoption of a blockchain-based criminal information management system holds the potential to revolutionize how criminal information is handled, stored, and shared. This innovative approach offers a secure, transparent, and decentralized platform that can significantly enhance the overall effectiveness, security, and transparency of the criminal information management system. Importantly, it prioritizes safeguarding the privacy and confidentiality of sensitive information. The integration of blockchain

technology represents a promising solution to address the challenges currently facing the existing criminal information management systems, ultimately contributing to the improvement of crime-fighting efforts.

The rapid increase in the number of criminal activities necessitates a fundamental shift in the way we manage criminal information. The limitations of conventional paper-based and centralized systems are becoming increasingly evident. The adoption of blockchain technology as a foundation for criminal information management offers a path towards heightened efficiency, security, and transparency. By implementing a blockchain-based system, we can strengthen the fight against crime while preserving the privacy and confidentiality of crucial data. This innovative solution holds significant promise in addressing the pressing challenges inherent in the current criminal information management landscape.

Implementing secure file management system

In the context of managing criminal information, Blockchain technology has emerged as a significant research focus due to its potential to revolutionize the field. As a response to this growing interest, our team has developed an effective and efficient blockchain-based criminal information system, which has been deployed to support the police department in Sri Lanka.

The management of criminal information systems involves the handling of a vast amount of data, including but not limited to forensic data, crime records, evidence, and FIR (First Information Report) documents [1]. This data encompasses various formats, such as documents, images, audio files, and video files. Ensuring the security and integrity of this critical information is more important. To address this challenge, we have implemented the InterPlanetary File System (IPFS).

The InterPlanetary File System (IPFS) serves as a fundamental component of our secure file management system. IPFS operates as a peer-to-peer file sharing system that enables users to access files from multiple computers across a decentralized network, rather than relying on a single centralized server. This approach offers

significant advantages in terms of data security and availability. It is a powerful technology to store and share immutable data within a decentralized network [3].

By utilizing IPFS, our system ensures that the criminal information, including documents, images, audio, and video files, is distributed across the network in a manner that makes it highly resistant to data loss and tampering. This not only enhances the overall security of the system but also contributes to the preservation of data integrity over time.

The implementation of a secure file management system for criminal information is a crucial step in modernizing law enforcement processes. Recognizing the ever-increasing volume and diversity of data, our team has leveraged blockchain technology and the IPFS to create an innovative solution. This approach enhances the security, availability, and integrity of critical criminal information. By embracing decentralized and peer-to-peer technologies, we are advancing the capabilities of the criminal information management system, ultimately assisting law enforcement agencies in their mission to maintain law and order while protecting sensitive data from unauthorized access and manipulation. This initiative represents a significant advancement in the field of criminal information management.

Aastha Jain, Soumyajit Das, Anand Singh Kushwah, Tushar Rajora, Shagun Saboo “Blockchain Based Criminal Information Management System”

In the realm of criminal information management, the vulnerabilities of a centralized database are of paramount concern. These vulnerabilities expose the system to various types of attacks, many of which can severely compromise the integrity and reliability of stored data. Among the most common threats faced are SQL injection attacks and Distributed Denial of Service (DDoS) attacks.

DDoS attacks pose a significant risk as they inundate the system, server, network, and available bandwidth with huge amount of traffic. The impact can range from temporary service disruptions to permanent hardware damage, with the potential for data loss in extreme cases. Such attacks underscore the critical need for robust security measures in data management systems.

SQL injection attacks, on the other hand, target the database itself by attempting to extract sensitive information stored within it. In centralized systems, the vulnerabilities to SQL injection can lead to data breaches and unauthorized access, posing serious security concerns. These vulnerabilities necessitate careful consideration when designing and implementing information management systems.

The decentralized nature of blockchain technology offers a compelling solution to address these inherent vulnerabilities. Blockchain's properties ensure resilience against both software and hardware errors, reducing the risk of data compromise. Its immutability, wherein once data is recorded, it cannot be altered or deleted, enhances data integrity. By adopting blockchain in the context of criminal information management, we can mitigate the risks associated with centralized databases, bolstering the security and reliability of the system [2].

Saha Reno, Shovan Bhowmik, Mamun Ahmed"Utilizing IPFS and Private Blockchain to Secure Forensic Information"

In the realm of securing forensic information, the utilization of a private blockchain system presents several advantages, although it comes with inherent limitations. A distinctive feature of private blockchains is their capacity to store lightweight textual information within individual blocks. However, when dealing with large and data-intensive files, such as images, audio recordings, or video data, these limitations become apparent.

To address the challenge of efficiently storing and managing heavyweight information, the InterPlanetary File System (IPFS) plays a pivotal role in the system architecture. When forensic data, including images, audio recordings, or video files, is uploaded to the network, IPFS facilitates this process by providing a unique cryptographic hash for each piece of data. This cryptographic hash serves as a digital fingerprint, uniquely identifying a specific piece of evidence within the system [4].

This hybrid approach, combining the capabilities of a private blockchain and IPFS, offers an effective solution for securing forensic information. While the private blockchain ensures the immutability and security of critical textual data, IPFS

enhances the system's ability to handle large files efficiently. By leveraging these technologies in tandem, the system achieves a harmonious balance between data security and storage scalability, making it a robust choice for safeguarding forensic information. This innovative integration of blockchain and IPFS demonstrates the adaptability of blockchain technology to address real-world challenges in forensic data management, ultimately benefiting law enforcement and investigative efforts.

Hsiao-Shan Huang, Tian-Sheuan Chang, Jhih-Yi Wu “A Secure File Sharing System Based on IPFS and Blockchain”

In the domain of secure file sharing systems, it is essential to recognize that blockchain technology, while offering numerous advantages, also presents certain limitations when it comes to storing large files or documents. These limitations stem from the fact that traditional blockchains are primarily designed to handle relatively small amounts of data efficiently. When confronted with the need to store extensive datasets, a more innovative approach is required.

To address this requirement for accommodating large volumes of data securely, a decentralized storage medium comes into play. This medium is realized through the utilization of the InterPlanetary File System (IPFS), which operates on a peer-to-peer protocol. In the context of this system, each stored file, whether it be a document, image, or any other form of data, is assigned a unique cryptographic hash based on the content of the file [3].

The incorporation of IPFS into the file-sharing ecosystem offers significant advantages. By distributing the storage of large files across a decentralized network of nodes, IPFS alleviates the inherent scalability constraints of traditional blockchains. This distributed approach not only enhances the system's capacity to handle extensive data but also strengthens data availability and redundancy, as multiple nodes may store identical content. Moreover, the use of unique content-based hashes ensures data integrity and allows for efficient retrieval of specific files from the network.

This hybrid system, which combines the strengths of blockchain technology for secure transactions and IPFS for efficient, scalable data storage, represents a noteworthy

advancement in the realm of secure file sharing. It overcomes the challenges associated with blockchain's limitations in handling large files, thereby expanding the applicability of blockchain-based systems to a broader range of use cases. This innovative fusion of IPFS and blockchain showcases the adaptability and synergy of decentralized technologies, offering a promising solution for secure, efficient, and scalable file sharing.

M. Dhulavvagol Praveen, S G Totad, Mahadev Rashinkar, Ribhav Ostwal, Suprita Patil, Priyanka M Hadapad “Scalable Blockchain Architecture using off-chain IPFS for Marks Card Validation.”

Within the context of this research paper, the primary focus is on enhancing the throughput and performance of an application by integrating the InterPlanetary File System (IPFS) with blockchain technology. This integration represents a strategic approach aimed at achieving superior performance metrics. By combining these two innovative technologies, a multifaceted optimization of the application's operations is realized, encompassing memory utilization, transaction latency reduction, streamlined transaction processing, and overall enhanced throughput.

The integration of IPFS into the system architecture plays a pivotal role in addressing several critical aspects of the application's performance. IPFS, standing for the InterPlanetary File System, is a cutting-edge storage file system that leverages Distributed Hash Table (DHT) technology. DHT serves as a foundational component in IPFS, enabling the system to effectively store and manage massive volumes of data within a decentralized and distributed environment. This decentralized approach fundamentally alters how data is stored and accessed, moving away from reliance on a central server to a peer-to-peer network. [5]

By adopting IPFS, the application not only optimizes its memory usage but also significantly reduces transaction delays. IPFS's capacity to distribute data across a network of nodes ensures that data retrieval and access times are minimized, contributing to a more responsive and efficient system. Additionally, the integration

minimizes transaction processing times, enhancing the overall efficiency of the blockchain-based system.

The huge increase in throughput is one of this integration's most important advantages. The application can manage a greater volume of transactions and data without encountering performance problems thanks to the integration of blockchain and IPFS technologies. This scalability is essential, particularly in situations where the validation of report cards or other processes entails a significant amount of data.

Randhir Kumar, Rakesh Tripathi “Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain”

The implementation of a distributed file storage and access framework, which leverages the InterPlanetary File System (IPFS) and blockchain technology, represents a significant advancement in data management and transaction integrity. In this research, we explore the profound impact of utilizing IPFS's content addressing mechanism on the integrity of transactions within the framework.

IPFS's content addressing mechanism plays a pivotal role in enhancing the reliability and resilience of transactions. At the core of this mechanism is the generation of a unique cryptographic hash for each piece of data stored within IPFS. This hash, derived from the content itself, serves as a digital fingerprint, making transactions highly secure and tamper-proof. As a result, the ownership and authenticity of transactions become unequivocally established, contributing to a robust and trustworthy system.

One of the key benefits of this integration is the assurance it provides regarding the reliability of transactions. By obtaining cryptographic hashes from IPFS for each transaction, the framework ensures that the data exchanged remains unaltered and secure throughout its lifecycle. This not only bolsters the trustworthiness of the system but also mitigates the risk of data manipulation or unauthorized access.

Furthermore, the use of IPFS content addressing aligns with the principles of blockchain technology, where data immutability and transparency are paramount.

Combining IPFS's content addressing with blockchain's distributed and decentralized ledger further reinforces the integrity of transactions. The resulting synergy ensures that the framework's users can confidently rely on the security and accuracy of their data exchanges. [6]

1.2 Research Gap

The current state of the criminal information management system in Sri Lanka reveals a pressing need for significant improvements. The existing approach to managing criminal files and records is a manual and centralized system. Therefore, faces considerable challenges in handling the massive amounts of criminal information generated. In addition to being ineffective, this manual technique creates weaknesses. One of the critical issues is the susceptibility of data to tampering and unauthorized modification by malicious users. This poses a direct threat to the integrity, confidentiality, and availability of the stored data.

To address these complex challenges, our research endeavors to pioneer a secure and innovative solution. We propose the implementation of a robust file management system within a blockchain-based criminal information management framework, enriched by the integration of the InterPlanetary File System (IPFS). By transitioning to a decentralized network architecture, we aim to overcome the limitations imposed by traditional centralized systems and establish a more secure and scalable infrastructure. The core advantage of this approach lies in the augmentation of data storage capacity through the utilization of IPFS, ensuring that the system can accommodate the escalating volumes of criminal information generated [7].

The pursuit of these objectives leads us to devise a range of solutions that address the fundamental issues plaguing the current system. Our foremost goal is to guarantee the confidentiality, integrity, and availability of critical documents and sensitive information. By migrating to a blockchain-based system coupled with IPFS, we seek to fortify the security and protection of these sensitive records. This transition will minimize the risk of data breaches and unauthorized access, safeguarding the integrity of the data against malicious tampering.

The table below which summarize existing system and secure file management system in decentralized network.

	Existing System (Manual/Centralized System)	Secure File Management System in Decentralized Network
Confidentiality	Low	High
Integrity	Low	High
Availability	Low	High

Table 1: Research Gap

The aims to bridge the gap in the current criminal information management system in Sri Lanka. By proposing a novel solution based on blockchain and IPFS technologies, we envision a future where criminal information can be managed securely, efficiently, and at a scale. This not only enhances the operational efficiency of law enforcement agencies but also upholds the principles of data confidentiality, integrity, and availability, ultimately contributing to the enhancement of the criminal justice system in Sri Lanka.

2. RESEARCH PROBLEM

The current approach to managing criminal evidence in Sri Lanka faces an array of complex challenges that impact the integrity, security, and efficiency of the system. The primary method involves storing criminal data on conventional computing devices or secondary storage media like pen drives, hard disks, and CDs. Unfortunately, this approach is far from optimal. It exposes the system to a host of issues, including unauthorized access. Centralized criminal information management systems are particularly vulnerable to data breaches, where malicious actors can gain access to sensitive data.

Another critical concern is the physical security of storage devices. These devices can be stolen or lost, potentially resulting in the compromise of sensitive criminal evidence. Furthermore, data entry in the current system is often prone to errors, leading to incomplete or inaccurate records. The absence of stringent data privacy measures raises ethical and legal questions, as confidential information may not be adequately protected.

Additionally, the operational cost of maintaining such a system is high, and the potential for misuse or abuse of access privileges remains a significant concern. The risk of data leakage looms large, particularly with the proliferation of electronic records. Criminal personal identification information (PII) is particularly vulnerable, raising significant concerns about identity theft and privacy breaches. [8] Moreover, the centralized nature of the system makes it a target for various types of cyberattacks, including SQL Injection, Distributed Denial of Service (DDoS) Attacks, and Data Breaches.

To address the multifaceted challenges presented by the current criminal information management system, we propose a comprehensive solution centered on the implementation of a secure file management system within a decentralized network, leveraging the power of InterPlanetary File System (IPFS) technology.

IPFS, as the InterPlanetary File System, offers a revolutionary approach to data storage and retrieval. Its content-addressable nature ensures the integrity and reliability of data.

Each piece of data is assigned a unique cryptographic hash based on its content, making tampering virtually impossible. By adopting IPFS within a decentralized network, data can be securely stored and efficiently retrieved without relying on centralized servers or vulnerable physical storage devices.

The decentralization provided by IPFS significantly reduces the risk of unauthorized access, data breaches, or the theft of physical storage media. Data privacy is enhanced, as access to sensitive information can be carefully controlled and monitored. Additionally, IPFS lowers the operational costs associated with data management.

Furthermore, the transition to this secure and decentralized approach safeguards criminal personal identification information (PII) and minimizes the risk of identity theft. Cybersecurity threats are mitigated, and the system becomes more resilient to cyberattacks.

In essence, the proposed solution represents a significant leap forward in addressing the challenges of the current criminal information management system. By harnessing IPFS within a decentralized network, we not only enhance data security, privacy, and integrity but also lay the foundation for a more efficient and robust criminal evidence management system that upholds the highest standards of confidentiality and reliability.

3. RESEARCH OBJECTIVE

3.1 Main Objective

The central aim of implementing a blockchain-based criminal records management system is to establish a secure, transparent, and tamper-proof platform for the storage and management of criminal records. This overarching objective encompasses several key elements that are critical to modernizing the criminal information management landscape.

First and foremost, the adoption of blockchain technology fundamentally transforms the way criminal records are stored. Unlike traditional centralized systems, where data is stored in a single repository, a blockchain-based system distributes the data across a decentralized and distributed network of nodes. This decentralization enhances the security and resilience of the records, making them far more robust against tampering, unauthorized access, or modification.

Additionally, this system is designed to enhance the efficiency of the criminal management process significantly. With all criminal records residing on a decentralized platform, law enforcement agencies, courts, and other relevant organizations can access the information quickly and effortlessly. By streamlining processes and minimizing administrative delays, the criminal justice system becomes more effective.

3.2 Specific Objectives

3.2.1 Secure File Management System in a Decentralized Network

The specific objective of implementing a secure file management system within a decentralized network is to ensure the confidentiality, integrity, and availability of criminal information. In traditional systems, files are often saved without additional security measures, leaving them vulnerable to unauthorized access and modification. To address these vulnerabilities, the proposal entails the implementation of a secure file management system within a decentralized network, specifically through a blockchain-based criminal information management system in Sri Lanka.

This system's core focus is to address the existing challenges by safeguarding the confidentiality, integrity, and availability of criminal records. It accomplishes this by leveraging the InterPlanetary File System (IPFS) along with cryptographic techniques for decentralization and enhanced security. [9] IPFS, designed as a peer-to-peer protocol, offers a more secure and efficient alternative for file storage, which is particularly valuable in criminal information management systems. Files are broken down into smaller pieces and distributed across multiple network nodes, ensuring redundancy and fault tolerance. Content addressing, based on hash values, further enhances security by obfuscating file locations.

By implementing this decentralized network, the system guarantees the tamper-proof and transparent storage of criminal information, reducing the risks of unauthorized access, data breaches, and information tampering. Access to these records is tightly controlled, restricted to authorized personnel who must adhere to secure authentication methods. [10]

3.2.2 Advantages of Blockchain-based Criminal Information Management Systems

The utilization of blockchain technology in criminal information management systems offers a myriad of advantages. It ensures the confidentiality, integrity, and availability of criminal records, reducing the risks associated with unauthorized access and data

breaches. Furthermore, it enhances the efficiency, accuracy, and cost-effectiveness of managing criminal information.

In comparison to centralized systems, which are relatively straightforward to control but vulnerable to attacks, decentralized technology distributes data among multiple entities. This distribution significantly reduces the vulnerability of centralized systems, enhancing data security and integrity. Blockchain's immutability ensures that once data is recorded, it cannot be altered or deleted, further improving data quality, and minimizing the possibility of unauthorized tampering.

The transparency inherent in blockchain technology also contributes to its advantages. Records are verifiable and traceable, making it easier to maintain the integrity of criminal information. Additionally, the efficiency gains associated with streamlined access and data retrieval processes result in cost savings and resource optimization.

In conclusion, the objectives encompass a holistic transformation of the criminal information management landscape. The specific measures proposed, such as the use of IPFS within a decentralized network and the adoption of blockchain technology, promise to address existing challenges comprehensively. These innovations not only enhance data security, privacy, and integrity but also lead to a more efficient, reliable, and cost-effective criminal information management system.

3.2.3 Implementing Cryptography for Enhanced Security

In certain scenarios, it is crucial to bolster the security of the token-based access system, especially to guard against potential malicious users who may attempt to exploit vulnerabilities and gain unauthorized access to confidential information. To mitigate such risks effectively, the implementation of robust cryptography algorithms becomes imperative. These cryptographic measures add an additional layer of protection to safeguard sensitive data.

3.2.4 Symmetric Encryption for Permanent File Storage

To ensure the secure storage of permanent files and documents within the IPFS, a symmetric encryption approach is adopted. This method involves encrypting the files using a shared key. The key itself is stored in a highly secure manner, minimizing the risk of unauthorized access. When a user needs to access a particular document, they are required to decrypt the file using the corresponding key. This process guarantees that only authorized individuals with the appropriate decryption key can access and view the contents of the file.

3.2.5 Secure File Sharing with Asymmetric Encryption

When files need to be shared between two parties, a robust asymmetric encryption technique is employed. The sender encrypts the file using the recipient's public key before sharing it through the IPFS network. This ensures that only the intended recipient, possessing the corresponding private key, can decrypt and access the file. Asymmetric encryption adds an additional layer of security during file sharing, as it makes the data unintelligible to anyone other than the designated recipient.

The utilization of cryptography in these ways significantly enhances the overall security and confidentiality of the token-based access system. It fortifies the system against potential threats, ensuring that even if a malicious user gains access to the token, the data remains protected and inaccessible without the appropriate decryption keys. By implementing both symmetric and asymmetric encryption, this approach achieves a robust balance between data security and accessibility, ultimately safeguarding the integrity and confidentiality of sensitive information.

4. METHODOLOGY

4.1 File Upload and Token Generation Process in the Criminal Management System

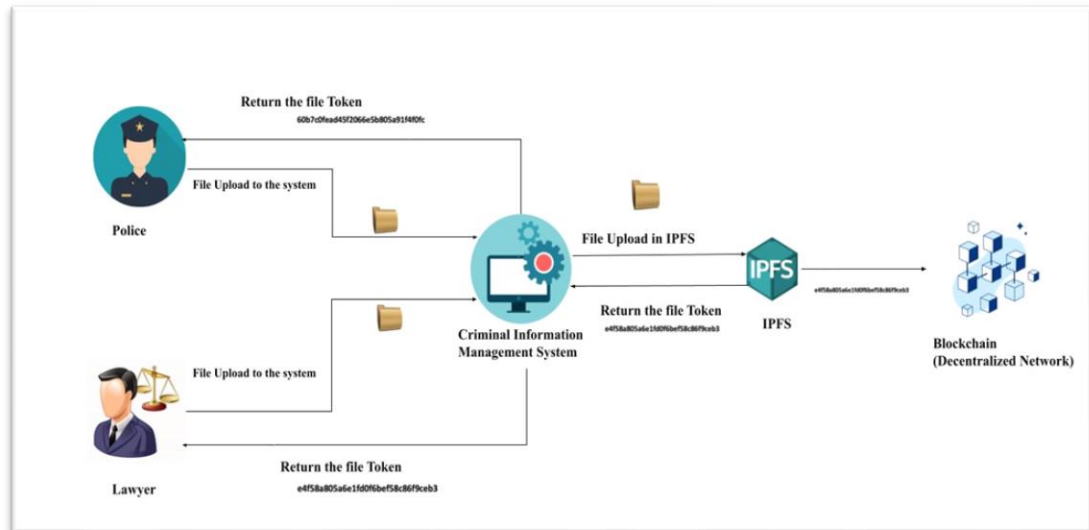


Figure 1: Secure File Management System

When a user initiates the process of uploading a file into the criminal management system, typically accessed via a web portal, the system is designed to accommodate various types of files, including audio, video, images, and more. Here's an in-depth breakdown of the steps involved:

- **User File Upload:** The user begins by uploading the file(s) into the criminal management system via the web portal. These files could encompass a wide range of formats and content, depending on the specific requirements of the system.
- **IPFS Integration:** Upon receiving the user's files, the system seamlessly integrates with the InterPlanetary File System (IPFS). IPFS is a peer-to-peer protocol designed for efficient and decentralized file storage and retrieval. The system transfers the uploaded files into IPFS for storage.

- **Unique Hash Generation - The Token:** As each file is transferred into IPFS, the system generates a unique cryptographic hash value for that specific file. This hash value serves as a distinctive identifier for the file within the IPFS network. Importantly, this identifier is often referred to as a “token.” It’s worth noting that this token is cryptographically derived from the file’s content, making it virtually impossible to replicate for any other file.
- **User and Blockchain Token Distribution:** The system takes two critical actions. First, it sends a copy of the generated token to the user who initiated the file upload. This user-specific token acts as a secure access key, allowing the user to retrieve and access the uploaded file in the future. Second, a copy of the same token is sent to the blockchain. This token is recorded on the blockchain’s immutable ledger, establishing a transparent and unalterable record of the file’s existence and associated access permissions.

The generated tokens play a pivotal role in enabling secure and efficient access to the uploaded files. With the possession of the appropriate token, anyone can access the corresponding file within the IPFS network. This mechanism ensures that files can be securely stored and efficiently retrieved while maintaining a clear audit trail on the blockchain for accountability and transparency.

and this process combines the advantages of IPFS for decentralized and secure file storage with the blockchain’s immutability to create a robust and transparent system for managing criminal data and file access.

4.2 Secure Storage of Criminal Information and Evidence

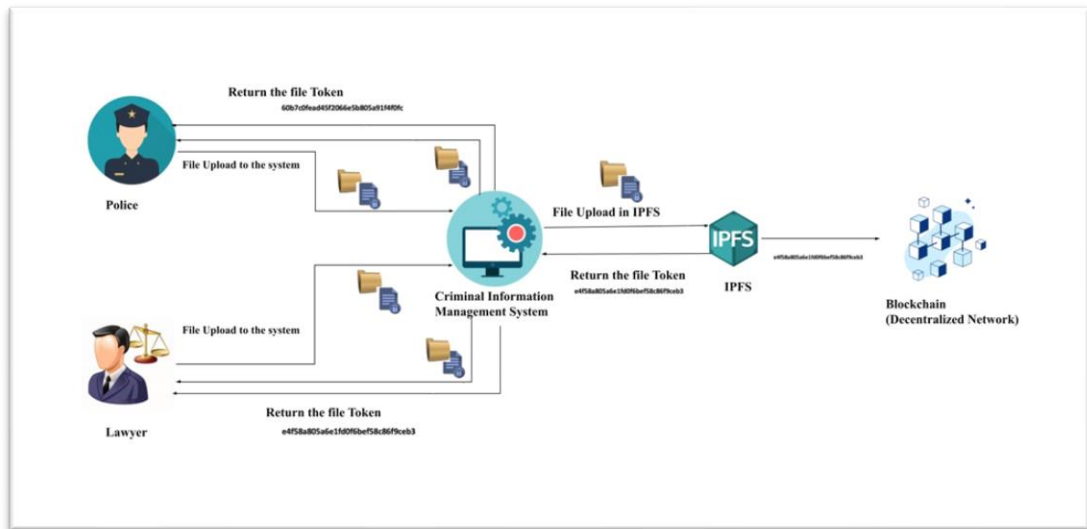


Figure 2: Secure File Management System to Store Files

In certain scenarios, it is imperative to maintain a permanent and secure repository for critical criminal information, forensic evidence, and crime-related data, ensuring their accessibility for future reference and legal proceedings. To achieve this, the files containing such sensitive information are stored in a cryptographically secure manner. Here's an in-depth look at the process involved:

- **Necessity of Permanent Storage:** There are instances in the realm of law enforcement and criminal justice where it becomes essential to preserve criminal information, forensic evidence, and crime-related data for the long term. This preservation is crucial for various purposes, including ongoing investigations, legal proceedings, historical records, and evidentiary support for potential future cases.
- **Cryptographically Secure Storage:** To meet the stringent security and confidentiality requirements associated with the storage of such sensitive data, a cryptographically secure approach is employed. This entails the use of advanced encryption techniques to protect the integrity and confidentiality of the files.

- **Symmetric Encryption:** One of the fundamental methods employed in this process is symmetric encryption. Symmetric encryption is a cryptographic technique where the same encryption key is used for both the encryption and decryption of a file. This key serves as the critical component that ensures only authorized parties can access and decipher the encrypted data.
- **Encryption and Decryption Using the Same Key:** To maintain data security and integrity, files containing criminal information, forensic evidence, and crime-related data are encrypted before being uploaded to the decentralized network. The encryption process transforms the file into an unreadable format that can only be restored to its original state using the corresponding decryption key. Importantly, this key must be securely stored and accessible only to authorized personnel.

By employing symmetric encryption, the system ensures that the same key is used for both encryption and decryption, guaranteeing that only individuals with authorized access and the requisite decryption key can retrieve and view the stored files. This level of security is paramount, as it safeguards the confidentiality and integrity of criminal data, forensic evidence, and crime-related information.

The utilization of cryptographic techniques, particularly symmetric encryption, provides a robust layer of security for the permanent storage of sensitive criminal information and evidence within a decentralized network. This approach aligns with the highest standards of data protection, ensuring that only authorized individuals can access and utilize the stored data while maintaining its integrity and confidentiality for future use in criminal investigations and legal proceedings.

4.3 Secure File Sharing Management System

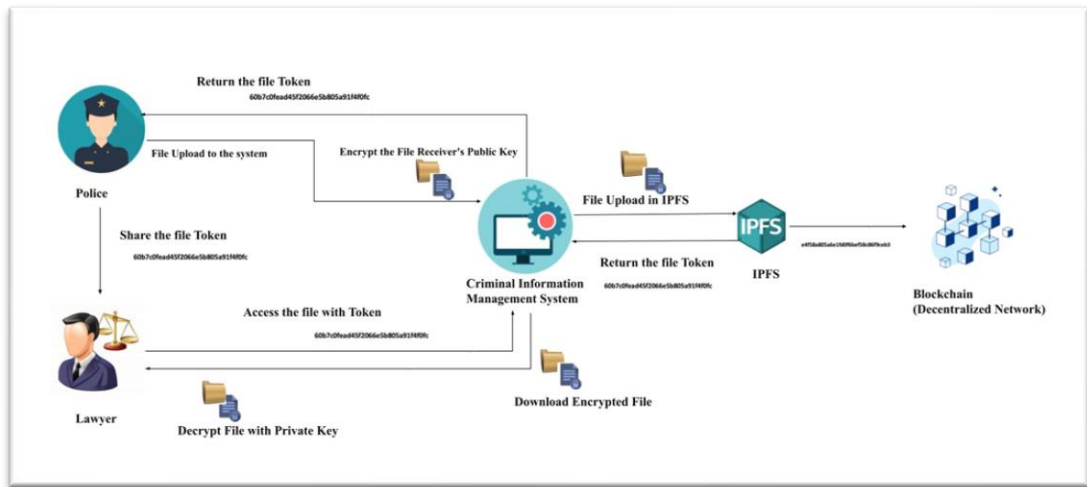


Figure 3: Secure File Management System to Share Files

In certain scenarios within the domain of criminal justice and law enforcement, it becomes essential to securely share critical information, including criminal data, forensic evidence, and crime-related evidence, with authorized individuals or entities. To ensure the confidentiality and integrity of these shared files, a cryptographically secure approach is employed. Here's an in-depth exploration of the process involved:

- **Necessity of Secure Sharing:** There are instances where it is imperative to share criminal information, forensic evidence, and crime-related data with specific recipients, such as law enforcement agencies, legal authorities, or other relevant parties. This sharing of information is essential for collaborative investigations, legal proceedings, and evidentiary support.
- **Cryptographically Secure Sharing:** To meet the stringent security and privacy requirements associated with the sharing of such sensitive data, a cryptographically secure method is adopted. This method ensures that the shared files remain confidential, tamper-proof, and accessible only to the intended recipients.
- **Asymmetric Encryption:** One of the fundamental cryptographic techniques employed in this process is asymmetric encryption. Asymmetric encryption, also known as public-key encryption, is a cryptographic approach where two

distinct but mathematically related keys are used (a public key and a private key). The public key is used for encryption, while the private key is used for decryption.

- **Encryption with Recipient's Public Key:** Before uploading the file into the decentralized network for sharing, it undergoes encryption with the recipient's public key. This ensures that only the intended recipient, possessing the corresponding private key, will be able to decipher and access the shared file. Importantly, this encryption process takes place before the file is transferred to the IPFS network, rendering it secure during transit and storage.
- **Decryption Using Private Key:** When the recipient initiates the download of the shared files using the provided token, a crucial step is required for access. The recipient must employ their private key to decrypt the file. This decryption process is essential for restoring the file to its original, human-readable format, making it accessible for viewing and analysis.

By leveraging asymmetric encryption, the system ensures that only the designated recipient, in possession of the private key, can successfully decrypt and access the shared file. This approach guarantees the confidentiality and integrity of shared criminal information, forensic evidence, and crime-related data, even during the sharing process.

The use of cryptographic techniques, specifically asymmetric encryption, provides a robust layer of security for the sharing of sensitive criminal information, forensic evidence, and crime-related data within a decentralized network. This approach aligns with the highest standards of data protection, ensuring that only authorized recipients can access and utilize the shared data while maintaining its confidentiality and integrity throughout the sharing process.

4.4 Development of a Criminal Information Management System

The development of a Criminal Information Management System (CIMS) is a complex and vital undertaking that necessitates a structured approach to ensure its effectiveness

and reliability. Here, we delve into the key aspects of implementing such a system, employing the agile software development life cycle:

- **Objective of the Criminal Information Management System:** The primary objective of the Criminal Information Management System is to create a comprehensive and efficient platform for the secure storage, management, and retrieval of criminal data, evidence, and related information. This system plays a critical role in supporting law enforcement agencies, legal professionals, and the criminal justice system.
- **Agile Software Development Life Cycle:** The development process of the CIMS follows the agile software development life cycle. Agile is a dynamic and iterative approach that prioritizes collaboration, flexibility, and continuous improvement throughout the development journey. This methodology is particularly well-suited to projects like CIMS, where requirements may evolve and adapt as the system takes shape.
- **Initiation and Requirement Gathering:** The development journey begins with an initiation phase, where the project's stakeholders define its scope, objectives, and expected outcomes. During this stage, the development team engages in requirement gathering. This involves a meticulous examination of the needs and preferences of end-users, including law enforcement agencies, investigators, and legal professionals. These requirements serve as the foundation upon which the system will be designed and built.
- **System Design:** Once the requirements are collected and prioritized, the system's design phase commences. During this stage, architects and designers create a detailed blueprint for the CIMS. This blueprint encompasses data structures, user interfaces, security protocols, and integration with necessary technologies. The design phase aims to ensure that the system will effectively meet the identified needs while maintaining scalability, security, and usability.
- **Implementation:** With the system's design in place, the development team proceeds to implement the CIMS. This phase involves writing code, configuring databases, setting up servers, and integrating various software components. The agile approach allows for incremental development, meaning

that the system is built and tested in manageable segments, facilitating early user feedback and adjustments as needed.

- **Testing and Quality Assurance:** Rigorous testing and quality assurance are integral to the development process. Comprehensive testing procedures, including unit testing, integration testing, and user acceptance testing, are carried out to identify and rectify any bugs, vulnerabilities, or issues. The goal is to ensure that the system functions as intended, meets performance benchmarks, and maintains data security and integrity.
- **Release and Deployment:** Following successful implementation and thorough testing, the CIMS is prepared for release and deployment. This involves making the system accessible to its intended users, whether they are law enforcement personnel, legal professionals, or other stakeholders. During this phase, training and support mechanisms are often put in place to facilitate a seamless transition to the new system.
- **Iterative Improvement:** The agile approach encourages ongoing improvement. After the initial release, the CIMS continues to evolve based on user feedback and changing requirements. Agile methodologies facilitate the incorporation of updates, enhancements, and new features to keep the system aligned with the evolving needs of the criminal justice landscape.

The development of a Criminal Information Management System is a dynamic and iterative process that prioritizes collaboration, flexibility, and responsiveness to changing requirements. By following the agile software development life cycle, the system can be designed, built, and improved to effectively support law enforcement, legal professionals, and the broader criminal justice system in their critical tasks.

4.5 Implementing a Secure File Management System

The integration of a Secure File Management System with the Criminal Information Management System (CIMS) is a critical step in enhancing the security and efficiency of managing criminal data, including FIR records, forensic evidence, and various

forms of crime-related information such as documents, audio files, video files, and images. Here's a comprehensive breakdown of this integration:

- **Objective of Integration:** The primary goal of integrating the Criminal Information Management System with the InterPlanetary File System (IPFS) is to establish a secure and efficient mechanism for storing, managing, and accessing critical criminal information. By leveraging IPFS, the system addresses key challenges related to data security, accessibility, and preservation.
- **Securing Criminal Information:** One of the primary benefits of this integration is the heightened security it offers for criminal data. The system ensures that sensitive information, including FIR records, forensic evidence, and various forms of crime evidence, is stored in a secure and tamper-resistant manner. This security extends to various file formats, such as documents, audio files, videos, and images, which are commonly used in criminal investigations.
- **Token-Based Access:** The Secure File Management System operates by generating a unique token for each uploaded file. This token serves as a secure access key, granting authorized users the ability to retrieve and access the associated file. Importantly, the token is cryptographically generated, making it virtually impossible to replicate or forge. It ensures that only individuals with the correct token can access the respective file.
- **Blockchain Integration:** Simultaneously with the generation of the token, the system sends a copy of this token to the blockchain. The blockchain serves as an immutable and transparent ledger that records the existence of each file and its associated token. This integration with blockchain technology adds an extra layer of security and transparency, as the file's access history is permanently recorded and cannot be altered.
- **User Interaction:** From a user perspective, the process is straightforward. When a user uploads a file into the system, they receive a unique token. This token acts as their secure passkey to access the file at any point in the future. The system ensures that the user retains this token securely, as it is the gateway to accessing the stored criminal information.

The integration of the Secure File Management System with IPFS and blockchain technology represents a significant step forward in ensuring the security, integrity, and accessibility of critical criminal information. It provides a robust solution for managing a variety of data types while maintaining transparency and accountability through blockchain-based record-keeping. This approach enhances the overall effectiveness and trustworthiness of the Criminal Information Management System, benefiting law enforcement agencies, legal professionals, and the criminal justice system.

4.6 Integrating a Secure File Management System with Blockchain

The integration of a Secure File Management System with blockchain technology represents a pivotal step in bolstering the security and reliability of data management, emphasizing the core principles of integrity, availability, and confidentiality. Here's a comprehensive breakdown of this integration:

- **Purpose of Integration:** The primary objective of integrating the Secure File Management System with a blockchain-based decentralized network is to fortify the data management infrastructure, with a focus on ensuring the utmost security and reliability. This integration is instrumental in upholding critical data principles, including integrity (data accuracy and trustworthiness), availability (data accessibility when needed), and confidentiality (data protection from unauthorized access).
- **Token-Based Data Handling:** Central to this process is the utilization of tokens generated by the Secure File Management System. These tokens serve as secure access keys to specific files within the system. When a user interacts with the system, such as uploading or retrieving a file, they are issued a unique token. This token is essential for subsequent access to the associated data.
- **Sending Tokens to the Decentralized Network (Blockchain):** As part of the integration, the generated tokens are transmitted to the decentralized network, which is facilitated by blockchain technology. The blockchain acts as an immutable and transparent ledger, recording and validating the existence and ownership of these tokens. By leveraging blockchain's distributed and tamper-

resistant nature, the system ensures that the tokens and, by extension, the associated data, remain secure and unaltered.

- **Ensuring Data Integrity:** One of the primary benefits of this integration is the assurance of data integrity. When data is stored within the decentralized network and linked to unique tokens, any attempt at unauthorized modification or tampering becomes exceedingly challenging. The immutability of blockchain ensures that once data is recorded, it cannot be altered without leaving an indelible trace.
- **Enhancing Data Availability:** Through the integration with blockchain, data availability is also improved. Users can confidently access their files knowing that the blockchain records the ownership and validity of their tokens. This means that authorized users can retrieve their data reliably and conveniently, contributing to the system's overall efficiency.
- **Safeguarding Data Confidentiality:** In addition to integrity and availability, data confidentiality is a paramount concern. The integration ensures that only authorized users with the correct tokens can access the associated data. This multi-layered security approach, combining tokens, blockchain, and encryption, safeguards sensitive information from unauthorized access.

Integration of a Secure File Management System with blockchain technology enhances the overall security and reliability of data management. It ensures the integrity, availability, and confidentiality of critical information, benefiting users, organizations, and systems that rely on secure data handling. This approach aligns with the highest standards of data protection, contributing to the trustworthiness and effectiveness of the integrated system.

4.7 Implementing Cryptography for Data Security

The incorporation of cryptography is a fundamental component of data security within the context of the Criminal Information Management System. This approach encompasses two critical aspects: securing files when storing them in the InterPlanetary File System (IPFS) and ensuring data confidentiality when sharing files via IPFS. Here's a comprehensive breakdown of these cryptographic processes:

4.7.1 Cryptographic File Storage in IPFS

Encryption for Data Protection

When storing files in IPFS, it is imperative to apply encryption to enhance data protection. Cryptographic algorithms, such as symmetric encryption, come into play during this process. Symmetric encryption using a single key for both encryption and decryption.

Encrypting the File

Before uploading a file to the decentralized IPFS network, it undergoes encryption. This cryptographic transformation renders the file unreadable without the corresponding decryption key. Symmetric encryption ensures that only authorized individuals with access to the decryption key can decipher and access the stored file.

Secure Key Management

A crucial aspect of this process involves the secure management of encryption keys. Safeguarding these keys is paramount, as they are essential for decrypting the file when needed. Proper key management practices ensure that only authorized parties possess the keys required to access the encrypted files.

4.7.2 Cryptographic File Sharing via IPFS

Secure File Sharing

Sharing files securely through IPFS, the implementation of cryptographic measures. Specifically, asymmetric encryption, also known as public-key encryption, is employed in this context. Asymmetric encryption using a pair of keys “a public key and a private key” for data security.

Encryption with Recipient’s Public Key

Before initiating the file sharing process, the sender encrypts the file using the recipient’s public key. This ensures that only the intended recipient, possessing the corresponding private key, can decrypt and access the shared file.

Decryption Using Private Key

When the recipient receives the encrypted file through IPFS, they must employ their private key for decryption. This cryptographic process restores the file to its original, human readable format, enabling the recipient to access and utilize the shared information.

Implementation of cryptography within the Criminal Information Management System serves as a cornerstone of data security. It involves symmetric encryption for safeguarding files stored in IPFS, ensuring that only authorized individuals can access the data. Additionally, asymmetric encryption is used to securely share files via IPFS, guaranteeing that only the intended recipients with the requisite private keys can decrypt and utilize the shared information. These cryptographic measures significantly enhance the confidentiality and integrity of criminal data, contributing to the overall security and trustworthiness of the system.

4.8 Technology Used in Project

To implement secure file management systems the following technologies used.

Technology	Use of Technology
Cryptography	It used to secure data in block
Smart Contract	It is self-executing contract with the terms of the agreement
Peer to Peer Network (P2P)	It used to communicate and share data among the nodes in blockchain
Application Program Interface (API)	It is enabling interaction between application and system
InterPlanetary File System	To secure store and sharing file
Java Script, Python, Solidity	Backend of the secure file management
HTML, CSS, PHP	Web Application front end

Table 2: Technologies

4.9 Software Specification

Developing a secure file management system for blockchain-based criminal information management systems necessitates a systematic approach. The plan involves adopting an agile software development life cycle, which is renowned for its flexibility and adaptability in managing complex projects. Here's a comprehensive breakdown of the software development process:

Requirement Gathering

- **Information Sources:** The first step is gathering comprehensive requirements. This involves sourcing information from a multitude of reliable channels, including research papers, blogs, articles, and interviews with relevant experts and stakeholders. These sources collectively provide the foundational knowledge necessary for building a blockchain-based criminal information management system.
- **User Needs:** In parallel, user needs and expectations are assessed, ensuring that the final system aligns with practical use cases and delivers tangible value to end-users.

Designing

- **Architectural Blueprint:** Based on the gathered requirements, the system's architecture is meticulously designed. This step involves creating a detailed blueprint that outlines the system's structure, components, data flows, and interactions.
- **User Interface (UI) and User Experience (UX) Design:** In addition to technical architecture, attention is paid to designing an intuitive and user-friendly interface to enhance the overall user experience.

Developing

- **System Implementation:** The development phase involves the actual creation of the blockchain-based criminal information management system. Developers translate the architectural design and user interface into functional software components.
- **Coding Standards:** Adherence to coding standards and best practices is paramount during this phase to ensure code quality, maintainability, and scalability.

Testing

- **Thorough Testing:** Rigorous testing procedures are conducted to evaluate the system's functionality, security, and reliability. Testing encompasses various aspects, including functional testing, security testing, performance testing, and user acceptance testing.
- **Issue Resolution:** Any identified issues or discrepancies are addressed promptly to ensure the system's robustness and adherence to requirements.

Release

- **Deployment and Delivery:** The system is released to production environments. Continuous integration and continuous deployment (CI/CD) practices, often associated with DevOps, facilitate seamless updates and enhancements to the system as needed.
- **Monitoring:** Post-release, the system is continuously monitored to detect and address any issues that may arise in real-world usage.

Maintenance

- **Ongoing Support:** Maintenance is an ongoing process that involves regular updates, bug fixes, and optimizations to ensure the system's stability and performance.

- User Assistance: A crucial aspect of maintenance includes providing user support and assistance, addressing user inquiries, and ensuring that the system continues to meet evolving user needs.

The software specification process for developing a secure file management system within a blockchain-based criminal information management system follows a structured agile software development life cycle. This methodology ensures that the system is built on a foundation of well-defined requirements, rigorous design, robust development, comprehensive testing, and ongoing maintenance. Ultimately, it aims to deliver a secure, efficient, and user-centric solution that aligns with both technical and user-driven requirements.

5. TESTING AND IMPLEMENTATION RESULTS AND DISCUSSION

5.1 Secure File Sharing in Decentralized Network

To ensure secure file sharing in decentralized network used asymmetric encryption. Also known as public key cryptography. is a cryptographic technique that uses a pair of keys, a public key, and a private key, to secure communications and data.

Public Key: This key is intended to be widely distributed and is used for encryption. Anyone can use the public key to encrypt data or messages.

Private Key: This key must be kept secret by its owner and is used for decryption. Only the person with the private key can decrypt the data or messages that were encrypted using the corresponding public key.

Asymmetric encryption plays a crucial role in securing digital information, ensuring confidentiality, authentication, and data integrity.

Results of Asymmetric Encryption

1. Encryption

- Step 01: Select the file which need to encrypt.

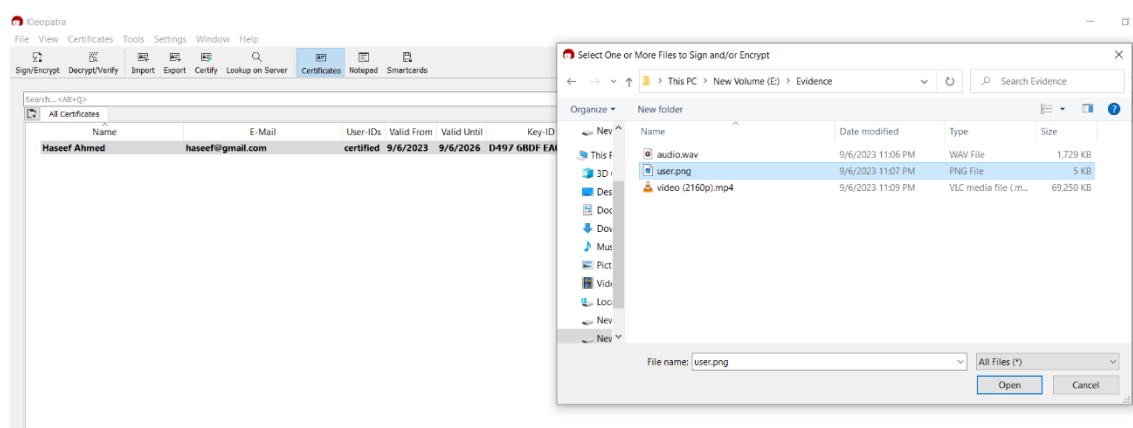


Figure 4: Asymmetric Encryption (Select File)

- Step 02: Select public key of the receiver to encrypt the file.

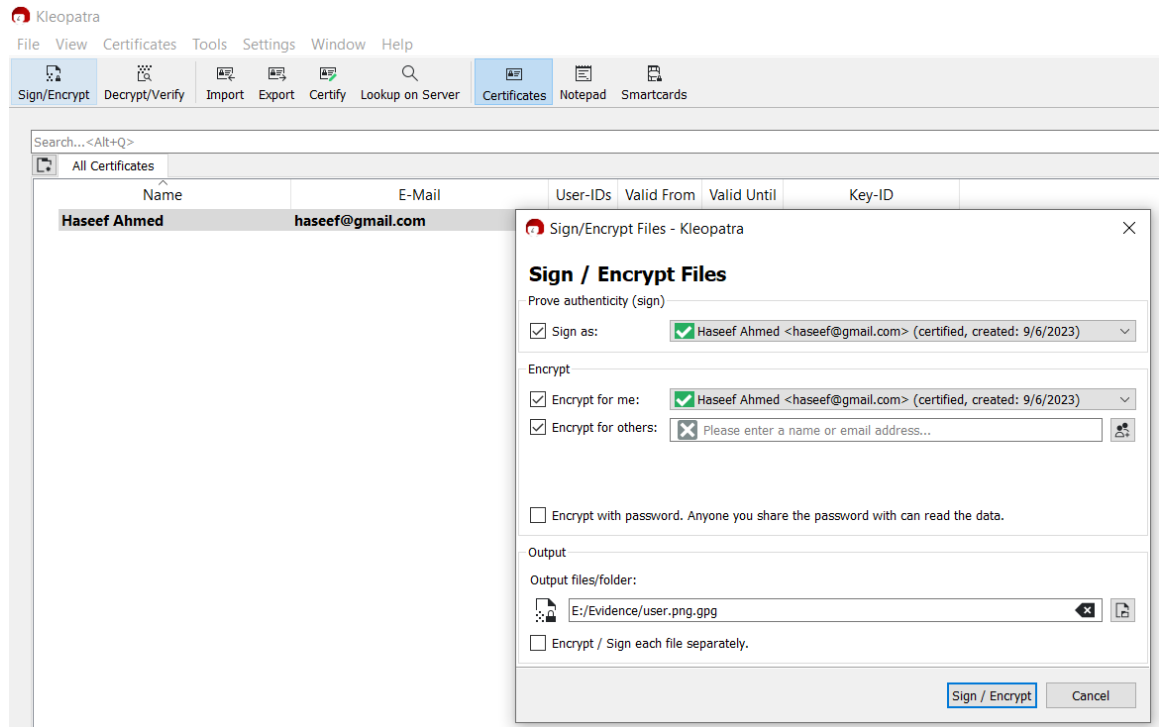


Figure 5: Asymmetric Encryption (Select Public Key)

- Step 03: Encrypt the file successfully.

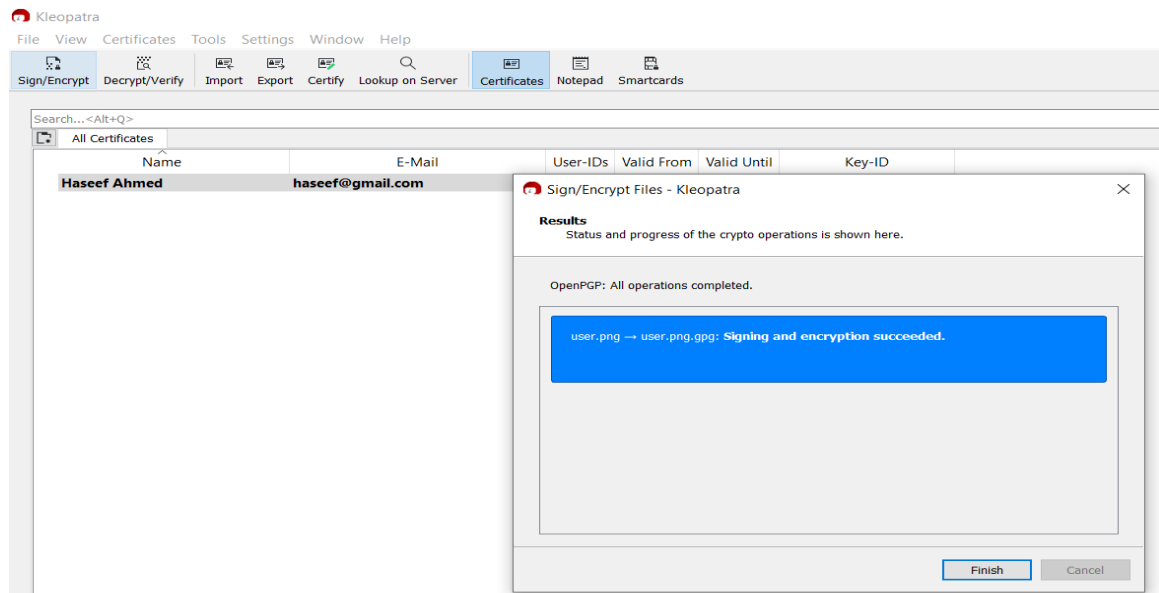


Figure 6: Encrypted Successfully

2. Decryption

- Step 01: Select Private Key to Decrypt the file.
- Step 02: Select File to Decrypt

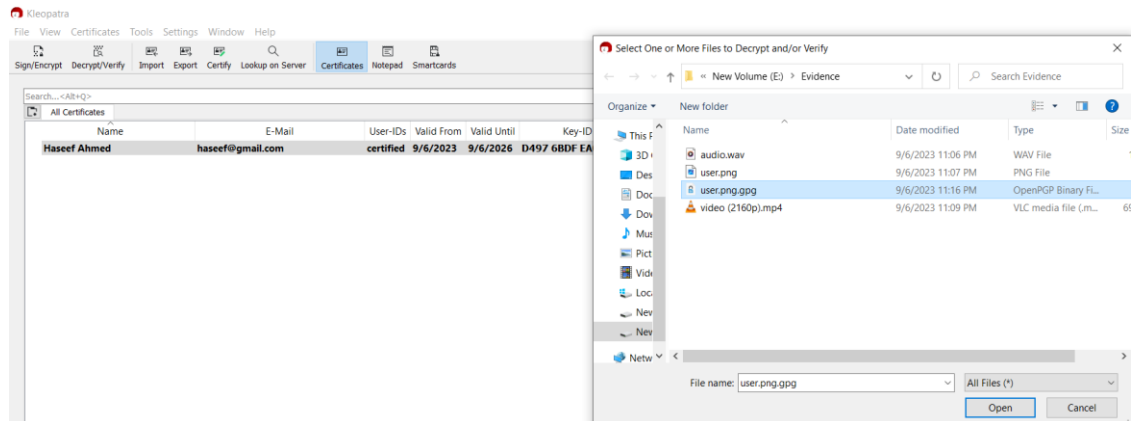


Figure 7: Asymmetric Decryption

- Step 03: Successfully file Decrypted.

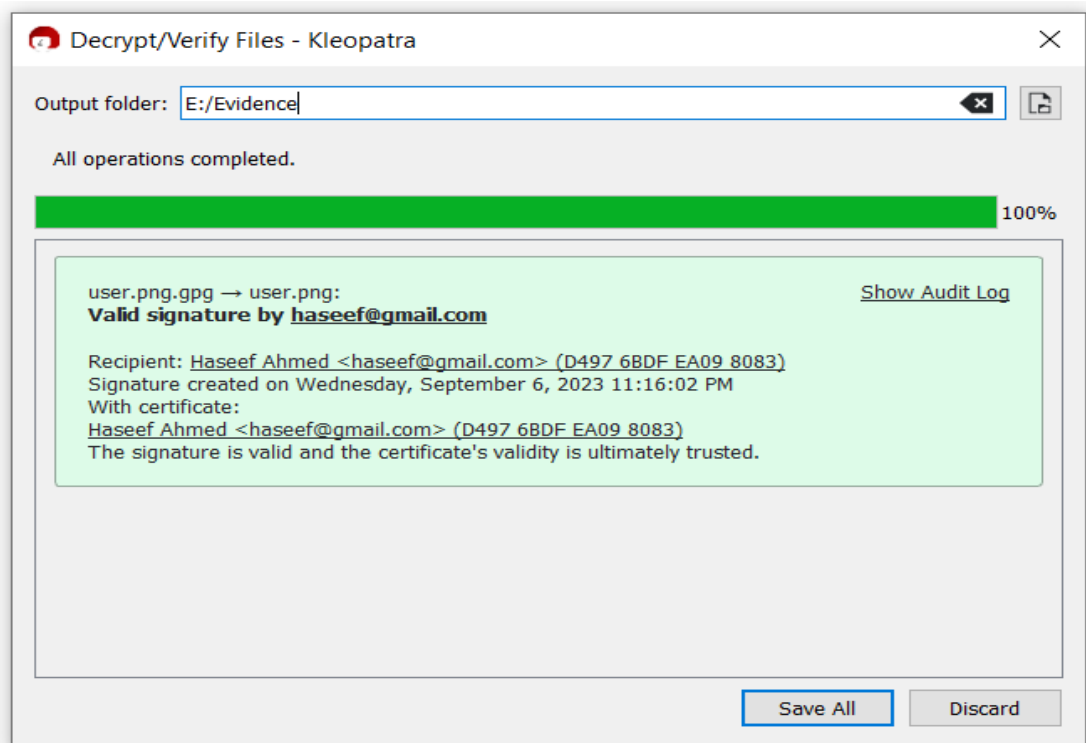


Figure 8: Successfully file Decrypted.

5.2 Secure File Management System in Decentralized Network

Secure File Management System in a Decentralized Network is a critical solution that ensures the confidentiality, integrity, and availability of files. For that used decentralized storage solution IPFS (Interplanetary File System) to store files in a distributed and censorship-resistant manner. Moreover, files are broken into smaller chunks and distributed across the network, making them resilient to data loss.

Results of Secure File Management

(Figure 9) which shows user interface of secure file management system, in here user can upload the file into IPFS and Download files from IPFS. When a user uploads a file, it needs to cryptographically encrypt to ensure only authorized person can access the file. And the file need to **“compressed to .zip.”** to ensure integrity of the file without having any data loss upload and download the file.

- Number 01 represents choose file from the device.
- Number 02 represents upload file to IPFS.
- Number 03 represents downloading the file from IPFS.

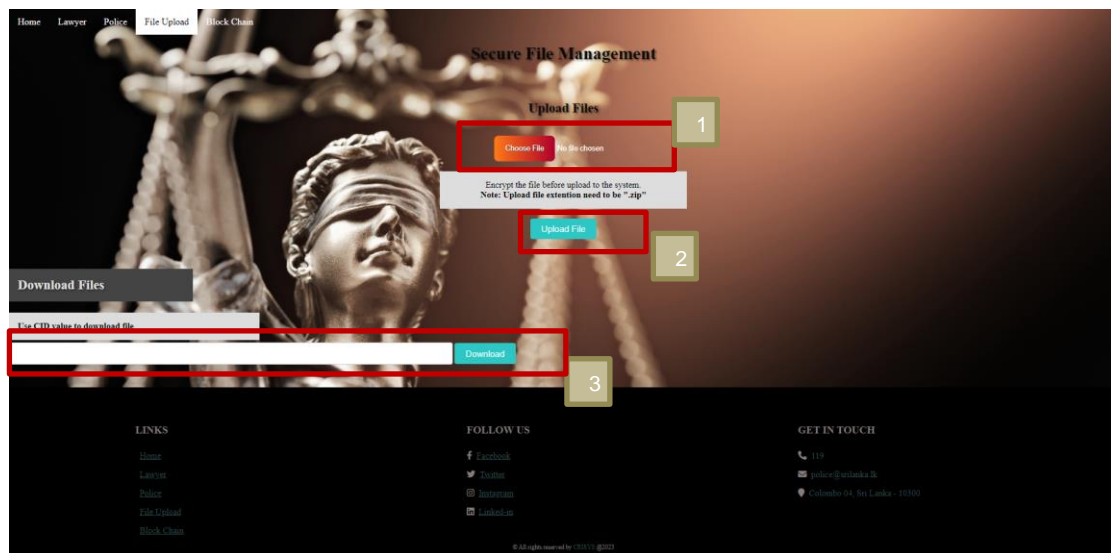


Figure 9: UI of Secure File Management

5.2.1 Upload Files to IPFS

When a user uploads the files into IPFS, the system generates a unique hash value, known as a Content Identifier (CID) or simply a hash, to represent the content of that file. This hash serves as a cryptographic fingerprint for the file and is used to retrieve and verify the content within the IPFS network.

When a user uploads a file to IPFS, the system breaks the file into smaller blocks or chunks. These blocks are typically 256 KB in size. Each of these blocks is hashed using a cryptographic hash function called SHA-256 (Secure Hash Algorithm 256-bit). This hash function takes the content of the block and produces a fixed-length hash value, which is a unique representation of the block's data.

IPFS uses a MerkleDAG (Merkle Directed Acyclic Graph) data structure to organize these blocks. In MerkleDAG, each block is represented as a node, and the links between nodes are based on cryptographic hashes. The hash of the root node of the MerkleDAG, which represents the entire content of the uploaded file, becomes the **Content Identifier (CID)** for that file. This CID is a unique identifier for the file's content.

One of the key benefits of using CIDs is that they provide cryptographic integrity verification. Because the CID is generated based on the content's data and structure, any alteration or corruption of the content will result in a different CID.

(Figure 10) which shows content identifier of the file which return from the IPFS, when user upload the file into IPFS using criminal information management system.

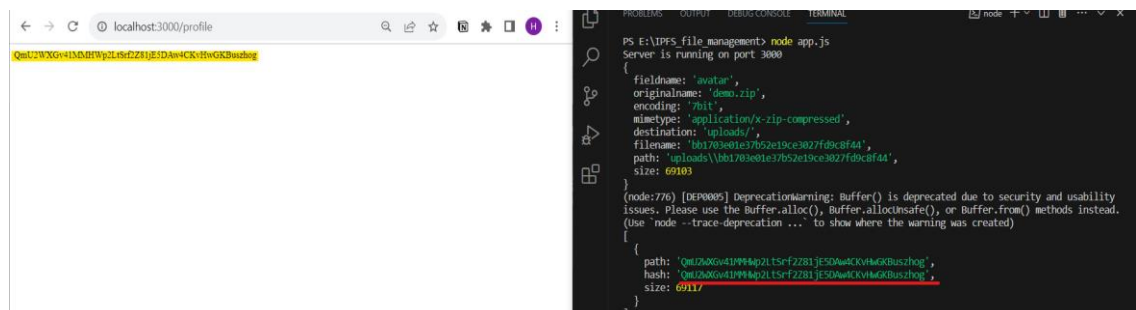


Figure 10: Upload Files to IPFS

5.2.2 Download File From IPFS

To download the file, it required to use CID value of the file. it is a unique identifier generated for each piece of content (file or data) added to the IPFS network. It is typically derived from the content itself, which means that the CID is generated based on the content's data. As a result, even a small change in the content will result in a completely different CID.

When you want to retrieve a file from the IPFS network, you don't need to know its location on any specific server or the IP address of a particular node. Instead, you use the CID associated with the file. Moreover, IPFS is a decentralized and distributed network where content is stored across multiple nodes (computers) in the network. It uses content addressing to locate the file. This means that the CID itself contains information about how to find the file within the IPFS network.

(Figure 11) it represents download file from IPFS with the help of CID value of the file.

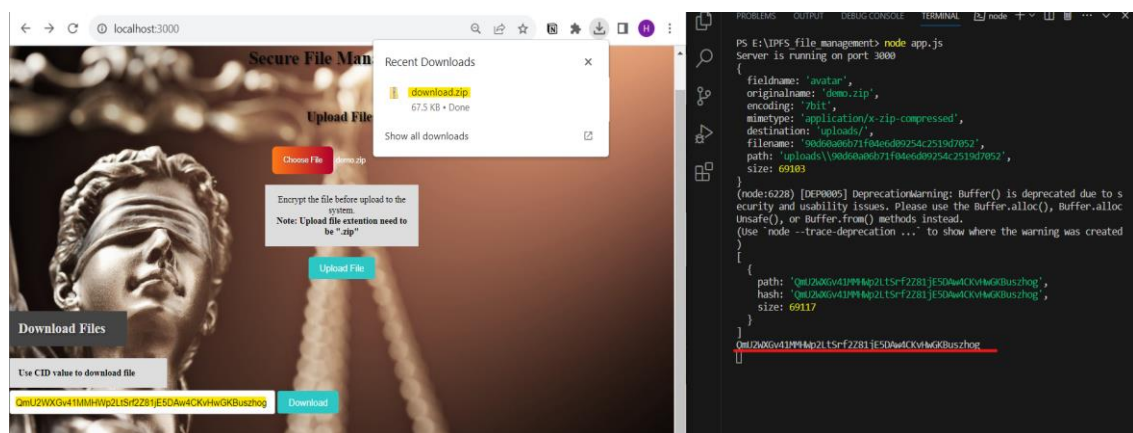


Figure 11: Download file from IPFS

5.2.3 Integrity Check of The File

Hash values are often used for this purpose because they are unique representations of a file's contents. Even a small change in the file would result in a significantly different hash value, with help of this hash value check integrity of the file.

Uploaded file hash

Observe hash value of the uploaded file.

```
PS E:\> Get-FileHash ".\demo.zip"

Algorithm      Hash                                          Path
-----
SHA256         589B727464E5C3069522A362E8CDD53E8268F955A5A11C08A79AC4D13D94D330  E:\demo.zip
```

Figure 12:Uploaded File Hash

Downloaded file hash.

Observed downloaded file hash value.

```
PS C:\Users\spt\Downloads> Get-FileHash ".\download.zip"

Algorithm      Hash                                          Path
-----
SHA256         589B727464E5C3069522A362E8CDD53E8268F955A5A11C08A79AC4D13D94D330  C:\Users\spt\Downloads\downlo...
```

Figure 13:Downloaded File Hash.

In secure file management system in decentralized network, when uploaded file into IPFS without it uploaded without any data lost of the file. At the same time when downloading the downloaded as it is without any data lost. It proved when uploaded file hash value and downloaded file hash vale both are same.

5.2.4 Send Token to Blockchain

Finally send CID value (Hash/Token) of the evidence was send into blockchain. The value send to the blockchain was manual method. When police officer entering a record, it required to enter evidence file, but in blockchain it store light weight of information such as records. Because of that used IPFS system to store file securely. With the help of that successfully store file and send that unique hash value into blockchain.

As an example, the evidence file belongs to this case/ incident.

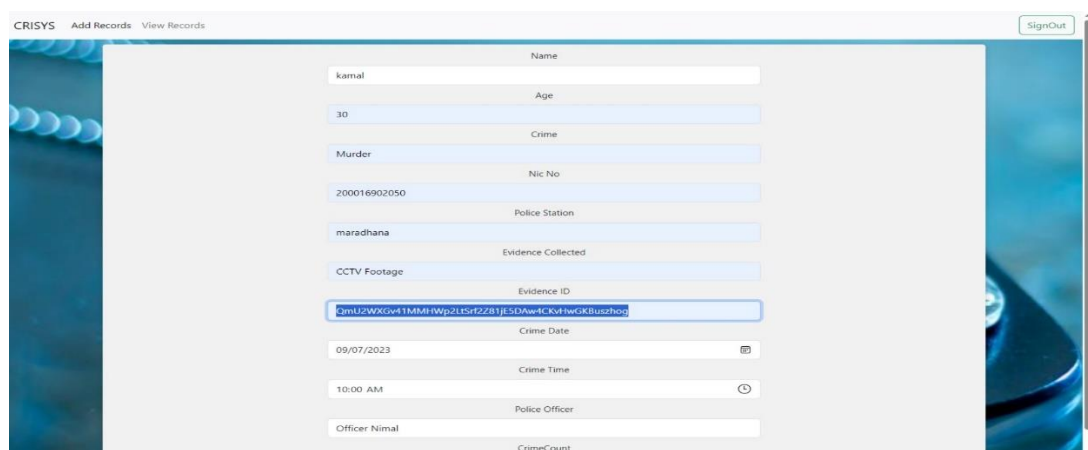


Figure 14: Send token to Blockchain.

(Figure 15) it represents the records are successfully stored in blockchain.



Name	Age	Crime	NicNo	PoliceStation	Evidence Collected	Evidence ID	CrimeDate	CrimeTime	PoliceOfficer	CrimeCount
kamal	30	Murder	200016902050	maradhana	CCTV Footage	QmU2WXGv41MMHwP2L1Sf2Z81jESDAw4CKvhwGKBuzhoo	2023-09-07	10:00	Nimal	3

Figure 15: Store CID value in Blockchain

6. COMMERCIALIZATION

A secure file management system in a decentralized network is a powerful system designed to safeguard sensitive data and restrict access to authorized individuals. Its value extends across various organizations that handle confidential information such as criminal information management systems, financial institutions, health providers, law firms, etc.

In addition, compliance with industry standards and regulations such as the Personal Data Protection Act, No. 9 of 2022 (PDPA) is crucial to ensure data privacy and build trust with clients.

To capitalize on the potential of a secure file management system, a method of profit should be established. One strategy is to seamlessly protect data by integrating the system into an organization's current infrastructure. To provide a positive user experience, maintenance services, customer support, and consulting services are also necessary. These services can help with any technical problem and provide you further information on how to use the system successfully.

Prepaid or postpaid choices are available for payment methods, and subscription periods can be hourly, monthly, or yearly. Because of this flexibility, organizations choose a payment option that fits their spending limits and frequency of use, making it a feasible investment.

In summary, a secure file management system is a useful resource for any organization that deals with sensitive data. Organizations may securely and successfully protect their sensitive data by following industry standards and regulations, providing maintenance and customer support services, and offering flexible payment alternatives.

7. CONCLUSION

In conclusion, in consideration of the increasing criminal activities, the study provided in this paper underlines the necessity and significance of reinventing criminal information management systems. The conventional paper-based and centralized approaches have proven inadequate, necessitating a paradigm shift. By embracing blockchain technology and leveraging the power of the InterPlanetary File System (IPFS) within a decentralized network, we have outlined an innovative and comprehensive solution. This approach enhances data security, integrity, and accessibility, while also addressing the unique challenges of managing large, sensitive criminal information.

Our proposed system not only strengthens the fight against crime but also safeguards the privacy and confidentiality of crucial data. It represents a significant advancement in the field of criminal information management, offering a potent defense against common threats and vulnerabilities. Furthermore, our integration of IPFS and blockchain technology showcases the adaptability of these decentralized technologies to meet the specific needs of forensic information management and secure file sharing.

Ultimately, the implementation of this distributed file storage and access framework has far-reaching implications beyond criminal information management. It exemplifies the potential of innovative technology combinations to enhance data integrity and reliability in diverse domains. In essence, our thesis underscores the importance of harnessing the capabilities of blockchain and IPFS within decentralized networks to create robust, trustworthy, and forward-looking data management solutions that meet the highest standards of security and efficiency.

8. REFERENCES

- [1] A. O. O. O. S. O. E. Onuiri, "A REAL-TIME CRIME RECORDS MANAGEMENT SYSTEM FOR NATIONAL SECURITY AGENCIES," in *Research Gate*, 2015.
- [2] S. D. A. S. K. T. R. S. S. A. Jain, "Blockchain-Based Criminal Record Database Management," in *2021 Asian Conference on Innovation in Technology (ASIANCON)*, PUNE, India, 2021.
- [3] T.-S. C. J.-Y. W. Hsiao-Shan Huang, "A Secure File Sharing System Based on IPFS and Blockchain," in *2020 2nd International Electronics Communication Conference*, 2022.
- [4] S. B. M. A. S. Reno, "Utilizing IPFS and Private Blockchain to Secure Forensic Information," in *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, Rajshahi, Bangladesh, 2021.
- [5] S. G. T. M. R. R. O. S. P. P. M. H. M. Dhulavvagol Praveen, "Scalable Blockchain Architecture using off-chain IPFS for Marks Card Validation," in *4th International Conference on Innovative Data Communication Technology and Application*, Hubballi, India, 2022.
- [6] R. T. R. Kumar, "Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain," in *2019 Fifth International Conference on Image Information Processing (ICIIP)*, Shimla, India, 2019.
- [7] M. C. H. G. S. T. Jignasha Dalal, "Verification of Identity and Educational Certificates of Students Using Biometric and Blockchain," in *Proceedings of the 3rd International Conference on Advances in Science & Technology (ICAST) 2020*, 2020.
- [8] A. G. G. U. Raveen Fernando, "Systematic Review on Existing Systems of Criminal Investigation Tracker with Suspect Prediction Algorithm & Criminal Records Management," 2021.
- [9] W. B. H. L. X. X. J. S. L. H. S. W. X. X. Y. X. Shaoliang Peng, "A peer-to-peer file storage and sharing system based on consortium blockchain," 2022.
- [10] A. R. P. M. F. A. K. F. T. M. A. K. Mamun Ahmed, "Using IPFS and Hyperledger on Private Blockchain to," *European Journal of Information Technologies and Computer Science*, 05 January 2023.