BLOCKCHAIN BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA

Project Id: TMP-23-270

Proposal Project Report

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

March 2023

BLOCKCHAIN BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA

Project Id: TMP-23-270

Proposal Project Report

M.N Haseef Ahmed

IT20157814

Supervisor - Mr. Kanishka Yapa

Co-Supervisor - Ms. Dinithi Pandithage

BSc (Hons) in Information Technology Specializing in Cyber Security

Department of Computer System Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

March 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

....   06/04/2023

(Mr. Kanishka Yapa)

Signature of the co-supervisor   Date

....   5/4/2023

(Ms. Dinithi Pandithage)

ACKNOWLEDGEMENT

I would like to express my sincere appreciation to the many individuals who have contributed to this project proposal.

First, I would like to thank Supervisor - Mr. Kanishka Yapa and express my gratitude to Co-Supervisor - Ms. Dinithi Pandithage and the Research Team for their contribution, support, and guidelines that have been invaluable in this development of research proposal.

ABSTRACT

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

Keywords: Blockchain, Criminal Records, IPFS, secure file, management system,

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATION

Abbreviation	**Description**
IPFS	InterPlanetary File System
CIMS	Criminal Information Management System
SQL	Structured Query Language
DoSS	Distributed Denial of Service
DHT	Distributed Hash Table
PII	Personal Identification Information
FIR	First Incident Report
API	Application Programing Interface

1 INTRODUCTION

1.1 Background

Due to the increasing number of criminal activities, there is a need to implement a more efficient and secure system to manage criminal information. One of the major problems with the traditional method of managing criminal information involves maintaining paper-based records that can cause loss or theft. Moreover, the information is stored in a centralized database. It has a lack of security, transparency, preservation of data integrity and consistency over time, which has led to unauthorized data modification and data breach. It can compromise the confidentiality and privacy of the information. [1]

To secure and transparent solutions for storing and sharing criminal records there can implement blockchain technology. It is a decentralized and immutable ledger that records transactions in a transparent and secure manner. Each block in the chain contains a hash of the previous block, which makes it virtually impossible to tamper with the data. The ledger is distributed across a network of nodes, there is no single point of failure, and the system has high protection against malicious activity.

In the blockchain criminal information management system each criminal record can be stored as a block on the chain, along with some metadata such as date, time location and type of crime. Only authorized persons can access the information, such as police officer, law enforcement agencies. With a secure authentication method. [2]

The implementation of a blockchain based criminal information management system potentially transforms how criminal information is handled, stored, and shared through the secure, transparent, and decentralized platform; it could enhance the effectiveness, security, and transparency of the system. While safeguarding the privacy and confidentiality of the information. It represents a promising solution for addressing the challenge facing the current system and improving the fight against crime.

1.2 Literature survey

1.2.1 Implementing Secure File Management System

In the criminal information management system Blockchain technology plays a major role as a research hotspot, because of that our team has provide an effective and efficient blockchain based criminal information system to the police department in Sri Lanka.

When thinking about information management systems, the system needs to handle a massive amount of data such as forensic data, crime records, evidence, FIR etc. [1] it can be documents, images, audio files, video files etc. to secure this information implementing IPFS.

IPFS (InterPlanetary File System) is a peer -to-peer file sharing system allowing users to access files from multiple computers on a decentralized network, rather than from a single centralized server. It is a most powerful tool for storing and sharing immutable data in a decentralized network. [3]

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

A centralized database may be vulnerable to many types of attack, most of which would seriously affect the integrity and reliability of the data. The common type of attack is SQL injection and DDoS attack.

DDoS attacks flood the system, server, network, and bandwidth sometimes resulting in permanent hardware issues and data loss can happen. SQL injection tries to reveal information in the database. Such as there can be issues in centralized system.

Decentralized properties of the blockchain ensure the inherent problems such as software and hardware error. It does not affect data integrity due to the immutable nature of the blockchain. [2]

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

Private blockchain can only store lightweight textual information inside the block. To store heavyweight information IPFS is utilized. When uploading images, audio, video data to the network and in return, the IPFS provides a cryptographic hash. This hash value can be used to identify a share of particular evidence. [4]

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

There are some limitations when storing large files or documents on the blockchain, to meet the requirement of storing large data. A decentralized storage media is produced. IPFS is based on a peer-to-peer protocol. Each store file is allocated a unique hash according to the content of the file. [3]

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."

In this research paper, to ensure throughput and performance of the application they integrate InterPlanetary File System (IPFS) with blockchain. Because of this integration it performs better optimizing memory, reducing transaction delay, reducing transaction processing and it ensures throughput.

IPFS storage file system that uses Distributed Hash Table (DHT) technology to store and manage massive volumes of data in a decentralized environment. [5]

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

IPFS content address increases the integrity of transactions by owning to the hash. It obtained from IPFS makes the transection reliable and resilient. [6]

1.3 Research Gap

The current criminal information management system in Sri Lanka is struggling to handle massive amounts of criminal information. The existing approach to managing criminal files and records is a manual and centralized system. Because that data can be changed and modified by malicious users, it is violating integrity, confidentiality, and availability of the data.

To address these challenges, implementing a secure file system for a blockchain based criminal information management system that utilizes IPFS (Interplanetary File System) in decentralized networks. IPFS-based blockchain data storage architecture has been developed to avoid the storage limit on the Blockchain. [7]

Because of that I came up with some solution to overcome that problem. That ensures confidentiality, integrity and availability of the documents and that sensitive information remains secure and protected.

	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

1.4 Research Problem

The current approach in Sri Lanka for managing criminal evidence involves storing the data on computers or secondary storage devices like pen drives, hard disks, and CDs. However, this approach is inadequate as it leads to several problems such as unauthorized access to centralized criminal information management systems, theft of physical storage, incomplete or inaccurate data entry, lack of privacy concerns, high cost, potential for abuse, and a high risk of data leakage. With the large number of electronic records, there is also a high risk of stealing criminal personal identification information (PII). [8] and centralized system vulnerable to many types of attack such as SQL Injection, DDoS Attack and Data Breach.

When implementing secure file management system in decentralized network it is using IPFS technology. By using this technology can overcome with this problem.

When it comes to the criminal information management system, all documents which are handled by the system, confidential information. Therefore, it is responsible to maintain confidentiality of the information.

2. OBJECTIVE

2.1 Main Objective

The main objective of a blockchain based criminal records management system is to provide a secure, storage platform that is transparent, tamper proof storage and managing criminal records. The use of blockchain technology can ensure that the records are stored in a decentralized and distributed manner, which makes them more secure and resistant to tampering or unauthorized modification.

Additionally, a blockchain based criminal records management system can also help to improve the efficiency of the criminal management system. By having all criminal records stored in a decentralized platform it is easily accessible, law enforcement agencies, courts, and other relevant organizations can quickly and easily access the information.

2.2 Specific Objective

To achieve the main objective, following specific objective need to be full fill.

Secure File Management System in a Decentralized Network: It ensures confidentiality, integrity, and availability of information.

In a traditional system when law enforcement or legal professionals upload files they are saved without any additional measures. It can be vulnerable to unauthorized access and modification.

Therefore, propose implementation of a secure file management system in a decentralized network, specifically a blockchain based criminal information management system in Sri Lanka. This system will address the existing challenges by ensuring the confidentiality, integrity, and availability of criminal records through the implementation of the Interplanetary File System (IPFS) with cryptography for decentralization.

Interplanetary File System (IPFS) was developed to address the issues of traditional centralized file storage systems. It is a peer-to-peer protocol that enables users to store and access files in a decentralized network. [9] IPFS is designed to provide a more secure, reliable, and efficient alternative for file storage. It can be especially useful in minimizing storage issues in criminal information management systems when storing criminal evidence. In IPFS, files are broken down into smaller pieces and distributed across multiple nodes in the network, ensuring that each node maintains a copy of the file, making it more resistant to failures or attacks. To identify files, IPFS uses content-addressing, which means that files are identified by their hash values instead of their location or path on the network.

By implementing a decentralized network, the system ensures that criminal information is stored in a tamper proof and transparent manner, which reduces the risk of unauthorized access, data breaches, and information modification. and can only be accessed by authorized personnel through secure authentication methods. [10]

Blockchain based criminal information management systems can address the challenges facing the current approach in Sri Lanka. The system ensures confidentiality, integrity, and availability of criminal records, reduces the risk of unauthorized access and data breaches, and increases the efficiency, accuracy, and cost-effectiveness of managing criminal information.

However, when compared to centralized systems, which are relatively easy to control but susceptible to attack, decentralized technology distributes data among multiple entities, reducing the vulnerability of centralized systems.

Implementing cryptography: in some cases, the token can be accessed by a malicious user and at that time the confidential information can be accessed, through the token. To mitigate that.

Implementing a cryptography algorithm.

- To store permanent files and documents in IPFS, implement symmetric encryption. To encrypt the file. And storing keys in a secure way. When a user needs to access the document there it is required to decrypt the file before access.
- When sharing the file between two parties the sender encrypts the file with receiver's public key and shares file through the IPFS, when receiver accesses the file, it is necessary to decrypt the file with receiver’s private key to access the file.

3. METHODOLOGY

3.1 Component Overview Diagram

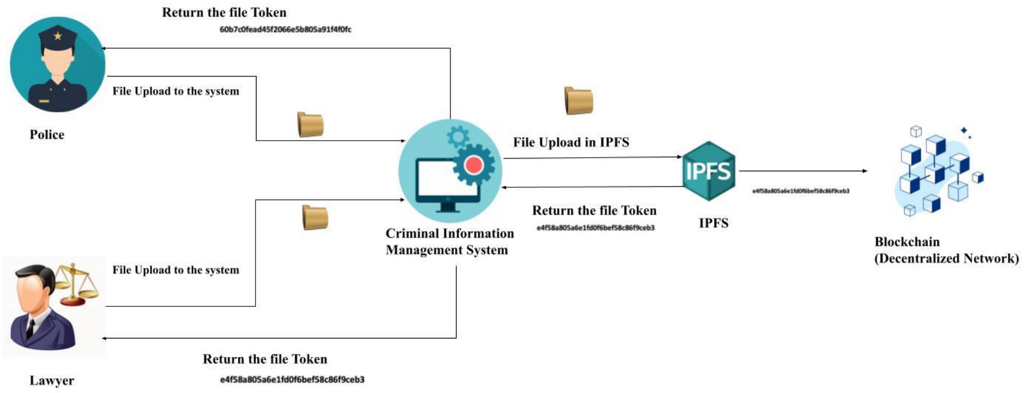
Return the file Token
60b7c0fead45f2066e5b805a91f4f0fc
File Upload to the system
Police
File Upload in IPFS
IPFS
e4f58a805a6e1fd0f6bef58c86f9ceb3
Return the file Token
e4f58a805a6e1fd0f6bef58c86f9ceb3
Criminal Information
Management System
IPFS
Blockchain
(Decentralized Network)
File Upload to the system
Return the file Token
e4f58a805a6e1fd0f6bef58c86f9ceb3
Lawyer

Figure 1:Secure File Management System

When a user uploads the file into the criminal management system (accessing system via web portal) the files can be audio, video, images etc. Then the system will send files into IPFS, and it generates a unique hash value to each file. It is called a token. And the copy of the token will be sent to the user. At the same time a token will be sent to the blockchain. With that token anyone can access the file.

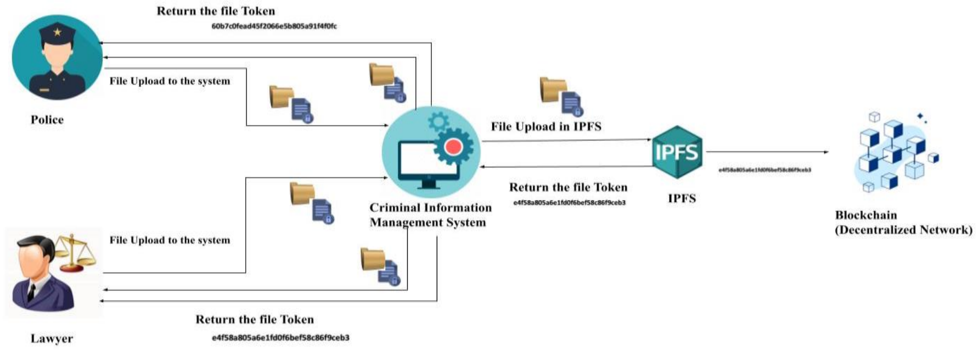
Return the file Token
60b7c0fead45f2066e5b805a91f4f0fc
Police
File Upload to the system
File Upload in IPFS
Criminal Information Management System
Return the file Token
e4f58a805a6e1fd0f6bef58c86f9ceb3
IPFS
e4f58a805a6e1fd0f6bef58c86f9ceb3
Blockchain (Decentralized Network)
File Upload to the system
Lawyer
Return the file Token
e4f58a805a6e1fd0f6bef58c86f9ceb3

Figure 2:Secure File Management System to Store Files

In some case there needs to store criminal information, forensic evidence, crime evidence permanently for future use. In that case files can store cryptographically secure. Before uploading the file into the decentralized network file needs to be encrypted (Symmetric Encryption) in this process to encrypt and decrypt the file using same key.

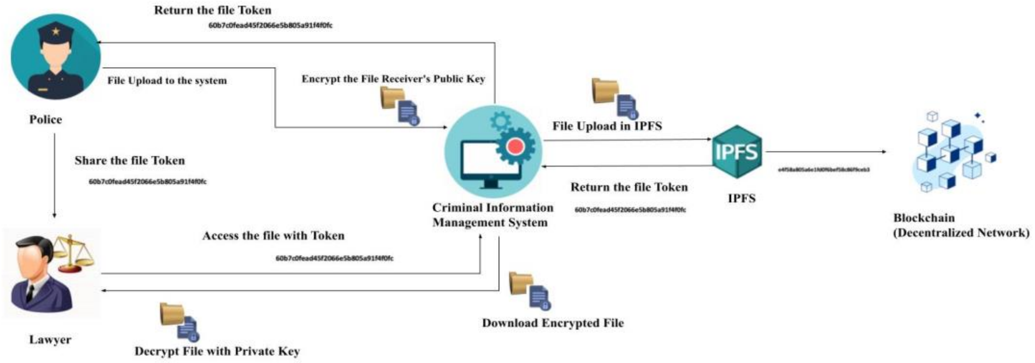
Return the file Token
60b7c0fead45f2066e5b805a91f4f0fc
Police
File Upload to the system
Encrypt the File Receiver's Public Key
File Upload in IPFS
Share the file Token
60b7c0fead45f2066e5b805a91f4f0fc
Criminal Information Management System
Return the file Token
60b7c0fead45f2066e5b805a91f4f0fc
IPFS
e4f58a805a6e1fd0f6bef58c86f9ceb3
Blockchain (Decentralized Network)
Access the file with Token
60b7c0fead45f2066e5b805a91f4f0fc
Download Encrypted File
Lawyer
Decrypt File with Private Key

Figure 3:Secure File Management System to Share Files

In some case there needs to be shared criminal information, forensic evidence, crime evidence. In that case files can be shared cryptographically secure. Before uploading the file into the decentralized network file needs to be encrypt with receiver’s public key (Asymmetric Encryption) and need to be upload, when receiver download the files using shared token, it required to decrypt the file with receiver’s private key and receiver can access the file.

Criminal Information Management System

Implementing a criminal information management system with a team. In this process we are following the “agile” software development life cycle. In the initial stage gathering some requirements according to the purpose and designing the system according to the gathered requirement and start implementing the system to archive the minestrone of the product. After successful implementation testing and releasing the system.

Secure File Management System

In this process integrating the criminal information management system with IPFS, because of this process can secure criminal information such as FIR records, forensic evidence, crime evidence it can be documents, audio, video, images etc. the secure file management system will create a unique token for each file. And it returns that token to the user at the same time it sends that token into the blockchain.

Integrate Secure File Management System with Blockchain

In this process the token, which is created by a secure file management system, sends to the decentralized network, because of this process there can ensure integrity, availability, confidentiality of the data.

Implementing Cryptography

- Implementing cryptography to store files in IPFS, to encrypt the file and to decrypt the file.
- And implementing cryptography when sharing files through the IPFS, to encrypt the file and to decrypt the file.

3.2.1 Technology Used in Project

To implement secure file management systems the following technologies, need to be used.

Technologies	**Use of technologies**
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 nods in blockchain
Application Program Interface (API)	It is enabling interaction between application and system
Interplanetary File System (IPFS)	To secure store and sharing file
Solidity, Java Script, Python	Programing languages

Table 2:Technologies

3.2.2 Software Specification

To develop a secure file management system for blockchain based criminal information management systems had a plan to use agile software development life cycle.

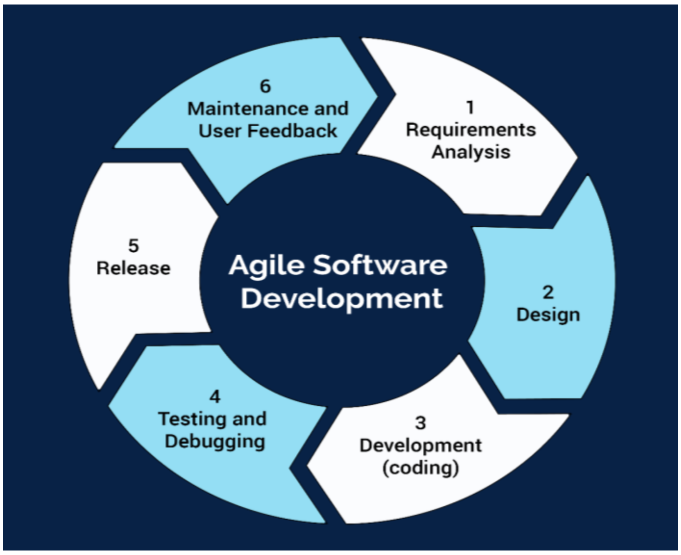

Figure 4:SDLC

Requirement Gathering: In this process gather information from research papers, blogs, articles, and by interviewing people gather information to build blockchain based criminal information management systems.

Designing: According to the gather requirement, architect and design the system.

Developing: Developing systems according to the gathered requirement and system architecture.

Testing: Testing the system if there was any issue or not and if it is properly integrated or not.

Release: Releasing the system it can update from time to time, the delivery method is DevOps.

Maintenance: Maintaining system properly

4. GANTT CHART

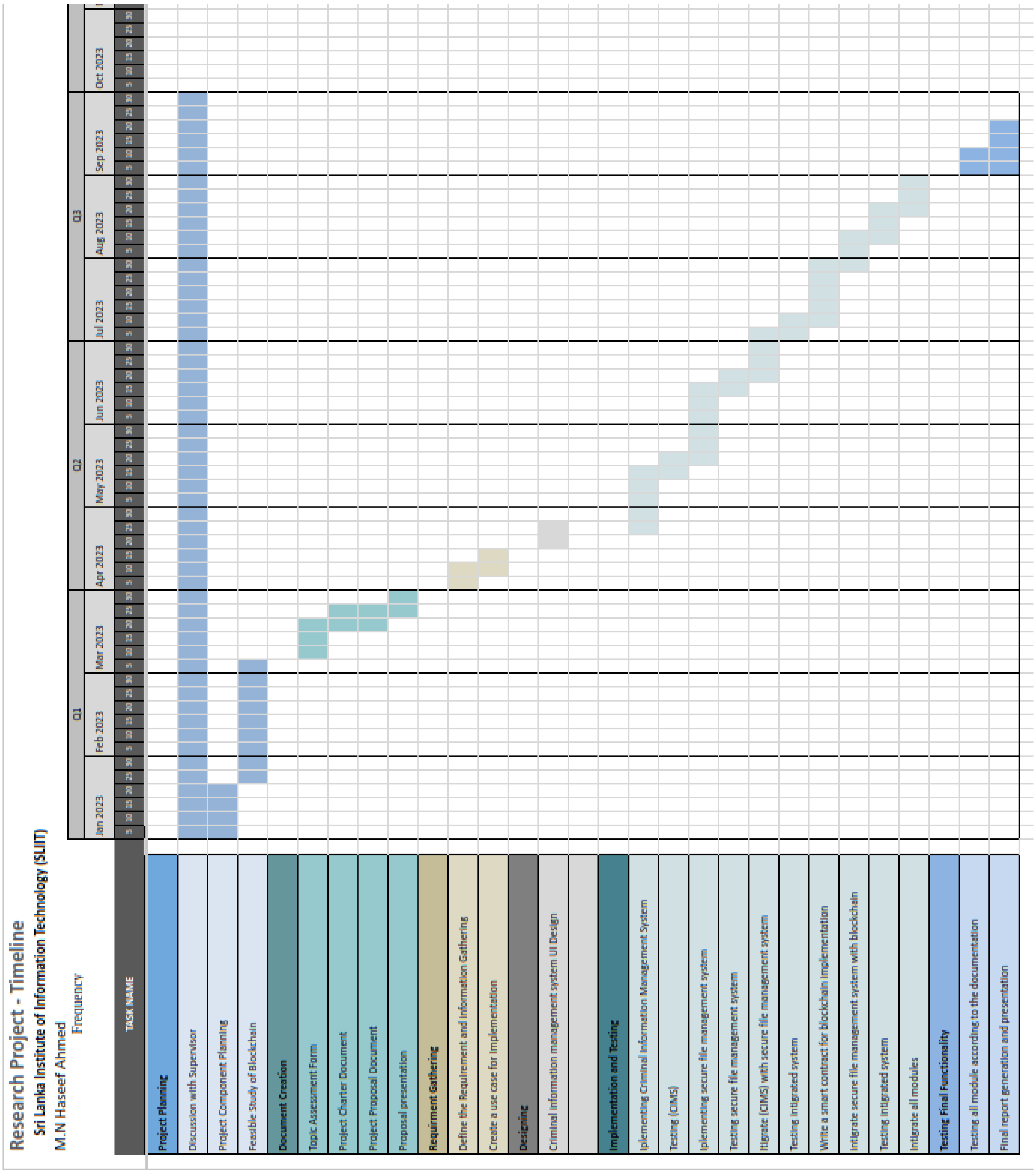

Figure 5:Gantt Chart

5. 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.

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.