BLOCKCHAIN-BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA

23-270

B.Sc. (Hons) Degree in Information Technology

Specializing in Cyber Security

Department of Computer Systems and Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

September 2023

BLOCKCHAIN-BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA

23-270

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

Department of Computer Systems and 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 acknowledgment of 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 acknowledgment is made in the text.

Also, I hereby grant to the Sri Lanka Institute of Information Technology the nonexclusive right to reproduce and distribute my dissertation, in whole or in part, in print, electronic or other mediums. I retain the right to use this content in whole or part in future works (such as articles or books)

Name	Student ID	Signature
Brahanawardhan B.	**IT20150952**	
Wijayarathne S. N	**IT20171438**	
Ahamed M. N. H.	**IT20157814**	
Thushitharan M.	**IT19983370**	

The supervisor/s should certify the proposal report with the following declaration.

The above candidates are carrying out research for the undergraduate Dissertation under my supervision.

Signature of the Supervisor

---------------------	---------------------
Mr. Kanishaka Yapa	Date

Signature of the Co-Supervisor

---------------------	---------------------
Ms. Dinithi Pandithage	Date

Abstract

As a result of Sri Lanka's current economic crisis, people there face difficult living conditions. Subsequently, crimes are rising fast. The country's criminal activity graph is continuously increasing due to the economic crisis and the globalization of cutting-edge technologies. As a secure and cost-effective method for maintaining a distributed database and keeping track of all kinds of digital transactions, blockchain applications are currently being investigated in various industries. The current criminal information management system in Sri Lanka employs a conventional paper-based approach. Storing, obtaining, and updating criminal records takes much time. Consequently, it has numerous negative effects. To mitigate the drawback, our team suggests using blockchain technology for a criminal information management system.

Every system and application requires login access, and since usernames and passwords are easier to hack, to increase security, all systems and applications have authentication systems as an additional level or level of security. Existing authentication systems have limitations, and with the development of technology, computational power, and, most importantly, Artificial Intelligence, these authentication systems are most likely to be exploited. In some situations, we have found that there are already authentication systems that have been exploited in the past.

This research is based on how and what has been done to improve the security that authentication systems bring as an additional layer or layers of security. We will investigate each factor individually and provide solutions and suggestions on how to improve these individual factors to a high level and, with that, bring the entire authentication system to a much higher level of security. This proposed system has three layers of protection with an additional features to enhance security.

Acknowledgment

We would like to take this opportunity to publicly express my gratitude to our mentors, Supervisor - Mr. Kanishka Yapa and Co-Supervisor - Ms. Dinithi Pandithage, as well as the entire research project team, for their unwavering support, excellent supervision, timely guidance, and inspirational leadership. We would like to express our sincere gratitude to everyone who contributed to this study. We would like to begin by expressing our appreciation to our supervisors for their guidance and support throughout the study process. When determining the general direction of this proposal, their insightful comments and suggestions were very helpful.

Additionally, we would like to express my gratitude to my friends and family members for showing us with the support and advice for the individual component that we have selected. With their input and suggestions, we were able to look into various different paths.

Finally, I (Senesh Wijayarathne) would like to express my gratitude to my friend and colleague Ms. M. W. N. L. De Silva [Masters in Information System Management - University of Colombo | B.Sc. (Hons) in Information Systems - General Sir John Kotelawala Defence University] who conducted a collaborative research with me that helped me with getting required data and details regarding the research topic that I have worked on.

***Keywords** - Blockchain, Two-Factor Authentication, Multi-Factor Authentication, 6-Digit Code, 6-Character Code, Criminal Records, Artificial Intelligence, One-Time Password*

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	**Description**
2FA	Two-Factor Authentication
MFA	Multi-Factor Authentication
AI	Artificial Intelligence
OTP	One-Time Password
SIM	Subscriber Identity Module
NIST	National Institute of Standards and Technology
HTML	Hypertext Markup Language
JS	JavaScript
CSS	Cascading Style Sheets
HMAC	Hash-based Message Authentication Code
BCIMS	Blockchain based criminal information management system
Dapp	Decentralization application
P2P	Peer to peer network
Baau	Blockchain as a unity
POS	Proof of service
SC	Smart contracts
TX	Transaction
pow	Proof of work
SHA-256	Secure Hash Algorithm 256-bit

1. INTRODUCTION

The world strives forward every day due to the information gathered by individuals who are dedicated to different sectors around the globe. This information that strives the world ahead can be collected by organizations, researchers, scientists, institutions, and law enforcement; these are just a few ways information can be gathered. A research done by professor David B. Hertz from the University of Miami and professor Albert B. Rubenstein from the Northwestern University have identified six varieties of information, and those recognized varieties of information are as follows [1];

1. Conceptual information: Information that is based on ideas, thoughts, hypotheses, hypotheses, etc., and could be used in the future or not. That does not always mean what you think it means. That information is not supported by science.

2. Empirical Information: Information obtained by experimentation or observation is referred to as empirical information. These facts are supported by science.

3. Procedural information: The approach that makes it possible for investigators to work more productively. The methods used to collect, modify, and test the investigation's data are referred to as procedural information.

4. Stimulatory information: Information that stimulates people's minds is referred to as stimulatory information.

5. Policy information: The decision-making process is the main emphasis of this kind of information. It is accessible through descriptions, images, diagrams, etc.

6. Directive information: Directive information is information that deals with giving guidance.

Digital, paper, and oral formats are the options for storing information. For information security and integrity, effective information management is essential. It includes the assortment, stockpiling, handling, and spread of data in a safe and effective way.

Different types of information will contain different levels of classifications; there are restricted, confidential, internal, and public levels of information. Depending on the individual, organization, or work sector, these information can be classified and can hold sensitive information.

If some information were to be disclosed or misused and that causes harm to organizations or individuals, those information can be known as sensitive information. Personal, financial, medical, and legal information holds sensitive information. For example,

- Identity theft or fraud can be executed by obtaining the personal information of an individual.
- Money laundering or embezzlement, generally known as fraudulent activities, can be conducted by obtaining an individual's financial information.
- Discrimination or blackmail is often executed by obtaining an individual's medical information.
- Legal information has the potential to undermine the justice system, jeopardize lives, and compromise ongoing investigations.

Information management is the organized, efficient arrangement, storage, processing, and transmission of information. It incorporates dealing with the data lifecycle, carrying out innovation to computerize data-related cycles, and creating approaches and methods to ensure the secrecy, integrity, and openness of data. In today's information-driven economy, effective information management is necessary for businesses to achieve their objectives and remain competitive [2].

An organization or an individual can accomplish a variety of objectives thanks to information management. It controls who can access important information, reduces risk, and improves compliance. Why effective information management is essential can be seen from the below-mentioned points,

- Controls the creation of records

- Ensures regulatory compliance
- Reduces operating costs
- Adopts new technologies
- Improves productivity and efficiency
- Reduces risks
- Protects proprietary information and preserves corporate memory

1.1. Background and Literature Review

According to ‘the morning newspaper,’ which was published in June 2022, crime within Sri Lanka has risen expediently [3]. Data collected from the Police Department of Sri Lanka shows that within the year 2021, there have been complaints and reports of 522 murders, 2263 robberies, and 6813 house break-ins, but the first four months of 2022 alone have received complaints and reports of 183 murders, 948 robberies, and 2224 house break-ins [3]. If we consider the provided information, we can see that there has been roughly a,

- 40% increment in murder compared to 2021.
- 68% increment in robberies compared to 2021.
- 31% increment in house break-ins compared to 2021.

The comparison between reported crimes in the first four months of 2021 and 2022 is shown in figure 1.1. 1,

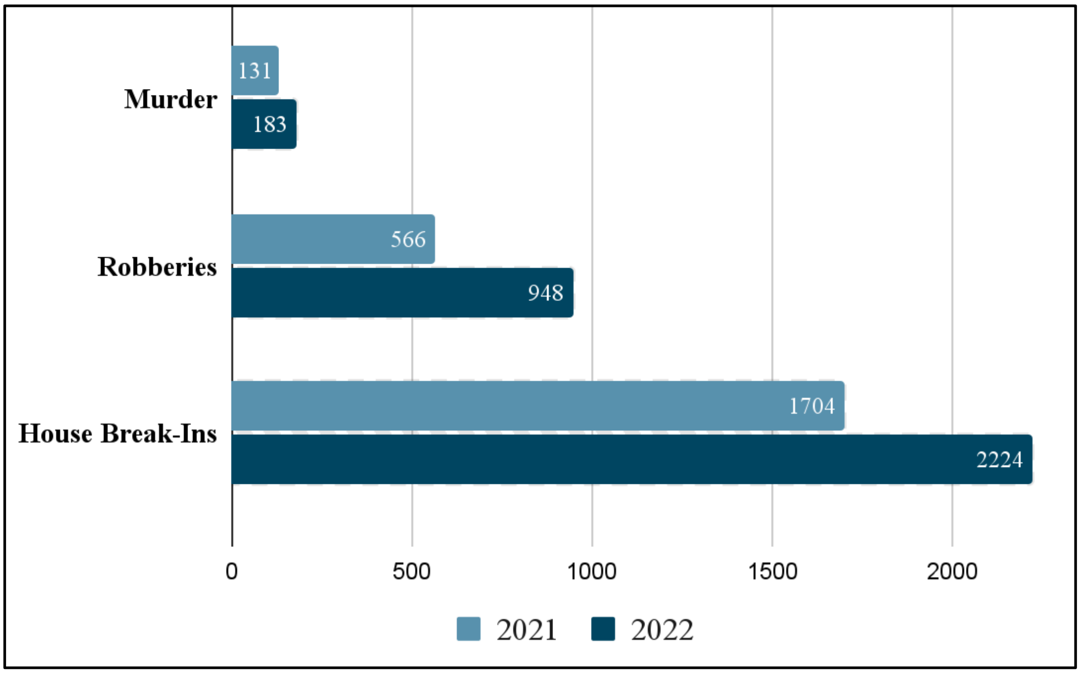


Figure 1.1. 1: Reported crimes in the first four months of 2021 and 2022

According to the data provided by The ‘Global Organized Crime Index’ Sri Lanka has been listed as a country with a 4.64 criminality score (110th of 193 countries, 33rd of

46 countries in Asia, and 6th of 8 countries in Southern Asia) and a 4.04 resilience score (129th of 193 countries, 28th of 46 countries in Asia, and 4th of 8 countries in Southern Asia) [4]. The numbers that were used to calculate the criminality score and the numbers that were used to calculate the resilience score are respectively shown in table 1.1. 1, and table 1.1. 2.

Criminality Score - 4.64	**Score**	**Final Score**
Human Trafficking	5.50	
Human Smuggling	6.00	
Arms Trafficking	5.00	
Flora Crimes	3.00	
Fauna Crimes	4.50	
Non-Renewable Resource Crimes	3.00	
Heroin Trade	6.00	
Cocaine Trade	3.00	
Cannabis Trade	5.50	
Synthetic Drug Trade	5.00	
Criminal Markets	**46.5**	**4.65**
Mafia-Style Groups	4.00	
Criminal Networks	5.00	
State-Embedded Actors	7.00	
Foreign Actors	2.50	
Criminal Actors	**18.50**	**4.63**
Final Total		**4.64**

Table 1.1. 1: Criminality Score of 4.64 in Sri Lanka

Resilience Score - 4.04		
	Score	**Final Score**
Political Leadership And Governance	4.00	
Government Transparency And Accountability	3.50	
International Cooperation	5.50	
National Policies And Laws	5.50	
Judicial System And Detention	3.50	
Law Enforcement	3.50	
Territorial Integrity	4.00	
Anti-Money Laundering	5.00	
Economic Regulatory Capacity	5.00	
Victim And Witness Support	3.00	
Prevention	2.50	
NON-STATE ACTORS	3.50	
Final Total		**4.04**

Table 1.1. 2: Resilience Score of 4.04 in Sri Lanka

These information about crimes that happen in Sri Lanka and who conducts these crimes are information that all police departments and stations around Sri Lanka should be aware of. In terms of our nation (Sri Lanka), the system for resolving complaints is run both manually and on a little computer. As a result, the system has several flaws, including a lack of accessibility, openness and worries about the security of sensitive information and the veracity of criminal records. Because of this, it has become difficult for law enforcement agencies to communicate information properly across several platforms and monitor and handle criminal processes.

Blockchain technology is a potential remedy for these drawbacks caused by criminal records that are collected and stored within Sri Lanka. In order to solve the issue, our team will suggest a "Blockchain-based Criminal Information Management System."

Blockchain is a distributed database that makes it possible for businesses to conduct safe, unalterable transactions. By harnessing the benefits of blockchain, a blockchain-based criminal information management system might offer greater security and transparency within a decentralized network, as well as increased efficiency in recording and managing criminal cases.

Unfortunately, research on the subject is limited, particularly in the Sri Lankan context, and the use of blockchain technology in the administration of criminal information is still in its infancy. In the context of the advantages, constraints, and practicality of a blockchain-based criminal information management system in Sri Lanka, this research attempts to evaluate its potential.

Considering previous research that was conducted on the general topic of Blockchain-based Criminal Information Management Systems, we can consider the following to be the tip of the iceberg,

- ‘Can blockchain strengthen the internet of things?’ by Nir Kshetri from the University of North Carolina, Greensboro [5].
    - According to Kshetri (2018), utilizing blockchain technology to validate a criminal suspect's identity might lower the likelihood of false arrests and improve the efficiency of criminal investigations.
- ‘Blockchain-Based Criminal Record Database Management’ by Aastha Jain, Soumyajit Das, Anand Singh Kushwah, Tushar Rajora, and Shagun Saboo from the Institute of Technology and Management, India [6].
    - Hash is a Mathematical operation that can convert an input of arbitrary length into an encrypted output of a fixed length. As a result, its unique hash value is always the same size, independent of the original data or file size.
    - On the other side, hashing is a one-way function that cannot be decrypted back to the original data. A system based on the SHA-256

mathematical algorithm (Secure hashing algorithm - 256). This methodology will prevent unauthorized access and confidentiality, Integrity, and Availability violation

1.2. Research Gap

According to our study, comparable Criminal Information Management systems have already been developed utilizing the blockchain idea, as was previously indicated during the literature review. All operations in Sri Lanka's criminal information management systems are conducted manually, relying on hand-filled forms and printed paper copies. Moreover, a centralized criminal information management system is used by certain of Sri Lanka's higher police departments. Specific criminal information management systems have a number of flaws. Any blockchain-based requirement to go through the public distributed ledger to complete some action. Current criminal information management systems must require enormous ledgers in order to perform some blockchain activities on their vast databases of criminal records.

This research is done by a group of four, and each individual will mainly focus on a different component of the research with gaps. Individually the four components that have been selected can be considered as four pieces of research, with each having its own merits. But, after the completion, there will be a final product with a blockchain-based criminal records management system to provide a secure, transparent, and tamper-proof platform for storing and managing criminal records. Following are the four individual components that were chosen to complete this research project to reach all its merits.

- Implementing smart contracts between criminal information management systems and blockchain technology.
- Implementing a Multi-Factor Authentication system for the Blockchain-based Criminal Information Management System.
- Implementing digital access control over the Blockchain-based Criminal records management System.
- Implementing a secure file management system in a decentralized network.

1.3. Research Problem

Picture a nation at a crossroads, where the ebb and flow of life has been profoundly disrupted by the tides of uncertainty. In the aftermath of a global pandemic, Sri Lanka faces a stark challenge—a surge in criminal activities that threatens the very fabric of society. The age-old systems for managing criminal information, tethered to stacks of paper and centralized control, stand ill-equipped to navigate this turbulent terrain. But there's a beacon of hope—a vision to revolutionize the way we understand, record, and combat crime. In the following chapters, we embark on a journey into the heart of innovation, where we explore the profound potential of blockchain technology to forge a more transparent, secure, and corruption-resistant Criminal Information Management System (CIMS) for Sri Lanka. Join us as we delve into the intricacies of this transformative endeavor, examining the intricacies of its design, its impact on data integrity and public trust, the efficiencies it introduces to law enforcement, and the roadmap it provides for a safer, more prosperous Sri Lanka.

1.3.1. Introduction to the Problem

In the aftermath of the COVID-19 pandemic, Sri Lanka has experienced a distressing surge in criminal activities, posing formidable challenges to public safety and the nation's overall well-being. Against this backdrop, the management of criminal information remains mired in antiquated, paper-based procedures, perpetuating inefficiencies and systemic vulnerabilities. Even in those select urban centers that have embraced computerized systems, centralized control persists, allowing corruption, political influence, and favoritism to infiltrate and erode the integrity of criminal records. This research problem addresses the urgent need to modernize and decentralize the management of criminal information in Sri Lanka, harnessing the transformative power of blockchain technology to combat corruption, bolster public safety, and lay the foundation for sustainable growth and progress.

1.3.2. Statement of the Problem

At its core, this research endeavors to design, develop, and implement a robust and transparent Blockchain-Based Criminal Information Management System (CIMS) in

Sri Lanka. This CIMS stands as a powerful antidote to the longstanding afflictions afflicting the nation's criminal information infrastructure, characterized by error-prone paper-based records and centralized data control. It seeks to revolutionize the manner in which criminal information is recorded, stored, and accessed, with a primary focus on eliminating opportunities for corruption, favoritism, and undue political influence. As a tangible first step toward this transformation, the research problem centers on the pilot implementation of the CIMS within the Colombo region.

1.3.3. Justification

The urgency of this research is underpinned by the profound consequences of inadequate criminal information management. The reliance on archaic paper-based records, replete with inaccuracies and vulnerable to manipulation, corrodes public trust and fosters an environment ripe for corruption and abuse of power. By embracing blockchain technology, Sri Lanka has a unique opportunity to establish an unassailable, transparent, and decentralized system for managing criminal information. This initiative resonates with the broader goals of the nation, which include a reduction in crime rates, restoration of public confidence, and the provision of a secure bedrock upon which to build societal and economic advancement.

1.3.4. Scope and Limitations

Though the ultimate aspiration is to implement the blockchain-based CIMS nationwide, the research astutely acknowledges the complexity and multifaceted challenges associated with such a sweeping transformation. Consequently, the initial phase of the project will concentrate its efforts on the Colombo region, serving as a pilot study. This localized deployment will facilitate a comprehensive evaluation of the system's feasibility, functionality, and impact. It is imperative to recognize potential constraints, encompassing infrastructural limitations, adoption hurdles, and regulatory intricacies, which may shape the successful expansion of the CIMS to encompass the entirety of the nation.

By undertaking this research problem, Sri Lanka is poised to confront head-on the burgeoning wave of criminal activities, dismantle the entrenched stronghold of systemic corruption, and empower its citizens with an innovative and transparent criminal information management system. The blockchain-based CIMS signifies a paradigm-shifting stride towards the realization of these goals, ensuring the safeguarding of public safety and the steering of the nation towards a more secure, prosperous, and promising future.

1.4. Research Objectives

"In the heart of Sri Lanka's pursuit of a safer and more transparent future, a transformative journey unfolds—one guided by innovation, integrity, and the power of blockchain technology. Against the backdrop of increasing criminal activities post-pandemic, our research endeavors to chart a path toward a Blockchain-Based Criminal Information Management System (CIMS) that is set to revolutionize how we record, manage, and protect crucial criminal information. As we delve into the following chapters, we invite you to explore three key objectives, each accompanied by its own set of groundbreaking components: the development of smart contracts for the blockchain, the implementation of a robust authentication system, the creation of a secure file management system, and the enhancement of the Chain of Custody process. These interconnected elements are poised to usher in a new era of efficiency, transparency, and trust within Sri Lanka's criminal justice system."

This introductory paragraph encapsulates the essence of your research journey, inviting readers to join in the exploration of the three key objectives and their associated components, emphasizing their potential to bring about transformative change in Sri Lanka's criminal information management landscape.

1.4.1. Development and Implementation of Blockchain-Based CIMS

Smart Contract for Blockchain: The development and implementation of a robust Blockchain-Based Criminal Information Management System (CIMS) involves the integration of smart contracts into the system architecture. Smart contracts, self-executing code stored on the blockchain, play a pivotal role in automating and securing various aspects of criminal information management. They ensure that predefined rules and conditions are met before transactions are executed, enhancing trust and efficiency in the system. For example, a smart contract could automate the process of recording new criminal incidents and securely storing them on the blockchain while validating the authenticity of the data source.

Authentication System: To ensure the integrity of the CIMS, a sophisticated authentication system is paramount. It not only safeguards user access but also verifies the identities of those entering data into the system. Blockchain technology can be employed to create a secure, decentralized authentication mechanism. For instance, a user's digital identity stored on the blockchain can be verified through cryptographic signatures, reducing the risk of unauthorized access and fraudulent entries into the system.

1.4.2. Ensuring Data Integrity and Transparency

Secure File Management System: A critical aspect of data integrity is the secure storage and management of files within the CIMS. The Secure File Management System is tasked with protecting sensitive criminal information from unauthorized access, tampering, or loss. Blockchain's inherent security features, coupled with encryption and decentralized file storage, can create an impenetrable fortress for these critical documents. For example, digital evidence files, court documents, and case reports can be stored securely on the blockchain, ensuring their integrity and accessibility to authorized personnel only.

1.4.3. Enhancing Efficiency and User Satisfaction

Chain of Custody: The Chain of Custody is a fundamental component for preserving the integrity of evidence and ensuring its admissibility in court. Blockchain technology can streamline the documentation of the Chain of Custody by creating an immutable and transparent record of evidence custody transfers. Each transfer event, from initial collection to courtroom presentation, is logged on the blockchain, reducing administrative burdens and the risk of mishandling. This, in turn, enhances the efficiency of the criminal information management process, ensuring the seamless flow of evidence and data.

By linking these four components with the research objectives, we create a comprehensive framework for the development and implementation of the blockchain-based Criminal Information Management System. Each component plays a vital role in achieving the overarching objectives, from automating processes with smart contracts to ensuring data integrity through secure file management, robust authentication, and maintaining the Chain of Custody. Together, these elements form the foundation for a transparent, efficient, and trustworthy system that addresses the core challenges of criminal information management in Sri Lanka.

2. METHODOLOGY

2.1. System Overview

The purpose of this system is to ensure the confidentiality, Integrity and Availability of Criminal Records in Criminal management system in Sri Lanka. The existing criminal system has so many drawbacks such as interoperability, scattered criminal records, violation of CIA, Handling with local databases, transparency of records, limited amount of accessibility, a lack of transparency, and concerns about critical data Security and the integrity of criminal records. This has made it challenging for law enforcement organizations to share information across various platforms and to monitor and manage criminal proceedings effectively.

A potential remedy for these drawbacks is blockchain technology. Therefore, our team is going to propose a "Blockchain based Criminal Information Management System" (CRISYS) to address the problem. Blockchain is a decentralized, decentralized database that allows for secure, accessible, and immutable transactions between organizations. A blockchain-based criminal information management system could provide improved security and transparency within a decentralized network, as well as increased efficiency in tracking and handling criminal cases, by utilizing the advantages of blockchain.

However, research on the subject is limited, especially in the Sri Lankan context, and the use of blockchain technology in criminal information management is still in its infancy. In the context of the benefits, challenges, and feasibility of a blockchain-based criminal information management system in Sri Lanka, this research aims to investigate its potential.

According to our Criminal system we developed the system using front-end development languages such as HTML, CSS, JavaScript and React JS. and the back-end development as Node JS, PHP. Here we moved into blockchain technology. We developed the blockchain using Ganache personal blockchain provided by truffle-suite.

Here are the Criminal system functionalities:

The Admin Officer: Once the Admin officer receives information about a crime, they enter the data into the system, which generates a block and eliminates the need for paperwork.

Validation Of Data: Once a block has been generated on the network, a copy is distributed to all network peers for verification and validation. If a block has been tampered with in any way within one peer network, it will not be authenticated by the rest of the network members. As a result, only verified data will be present on the network.

Availability of criminal data across the peer-to-peer network: Once the data has been validated by the miners, it is stored permanently on every blockchain node. Since the data is stored immutably, it is considered verified and authenticated, which allows people to access the data from anywhere with ease.

Access Data: Authorized individuals can access the data using a unique case ID and the associated hash.

Steps for the Blockchain Implementation

1. **Determine the Problem** – In Sri Lanka Police departments are depending on a local database and paper basis system to address these issues and implement smart contracts with the Encryption for Criminal Information Management System.
2. **Choose a blockchain platform** – Ethereum blockchain platform for implementing decentralized networks for our proposed system.
3. **Define the smart contract –** Define the rules and logic and behavior of blockchain based smart contact for the criminal system. Which includes specifying the inputs, outputs, and state variables of the contract.
4. **Write the smart contract code –** Use a solidity programming language supported by Ethereum blockchain platform to write the code for smart contract.

5. **Test the smart contract** – use testing framework and tools to test the functionality and security of smart contract. This includes unit testing, integration testing and security testing.
6. **Deploy the smart contract** – Deploy the smart contract for Ethereum blockchain platform using the appropriate deployment tools and processes. verify the correctness of the deployment and record the contract's address.
7. **Interact with the smart contract. -** A smart contract is a self-executing contract that is stored on the blockchain. It can be used to automate a variety of tasks, including adding new criminal records, updating existing information, or querying the database.A transaction is a unit of data that is exchanged on the blockchain. It can be used to transfer funds, add new data to the blockchain, or execute a smart contract. Ethereum is a blockchain platform that supports the execution of smart contracts. It is the most popular blockchain platform for developing and deploying smart contracts. A function is a block of code that performs a specific task. Functions are used in smart contracts to automate tasks such as adding new criminal records, updating existing information, or querying the database.
8. **Monitor and maintain smart contracts -** As the Criminal Information Management System (CIMS) evolves or security threats change, the smart contract may need to be updated. Smart contract developers should be prepared to implement necessary modifications while ensuring backward compatibility and data integrity. The contract's address and its transaction history are recorded on the Ethereum blockchain. This information provides transparency and an immutable ledger of all interactions with the smart contract, which facilitates accountability and auditing.

2.1.1. Secure File Management System in Decentralized Network

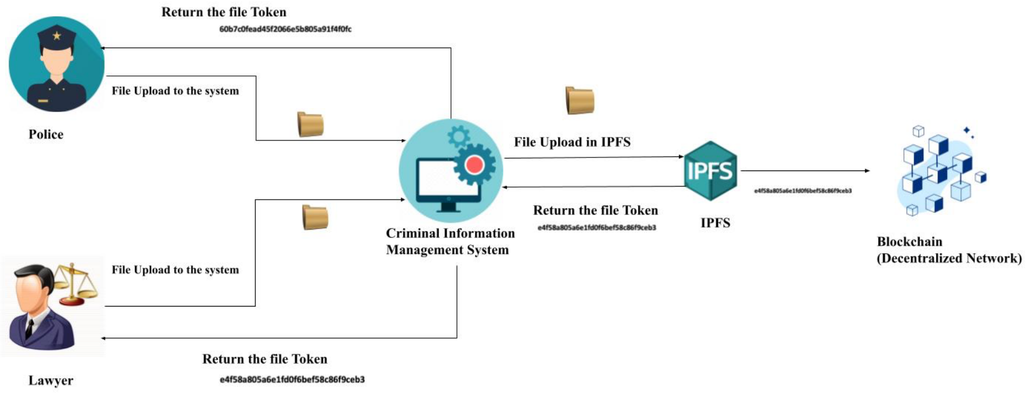

Return the file Token
60b7c0fead45f2066e5b805a91f4f0fc
File Upload to the system
Police
File Upload in IPFS
IPFS
e4f58a805a6e1fd0f6bef58c86f9ceb3
Return the file Token
e4f58a805a6e1fd0f6bef58c86f9ceb3
IPFS
Criminal Information
Management System
Blockchain
(Decentralized Network)
File Upload to the system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

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:

1. 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.
2. 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.
3. 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.
4. User and Blockchain Token Distribution: Simultaneously, 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.

Secure Storage of Criminal Information and Evidence

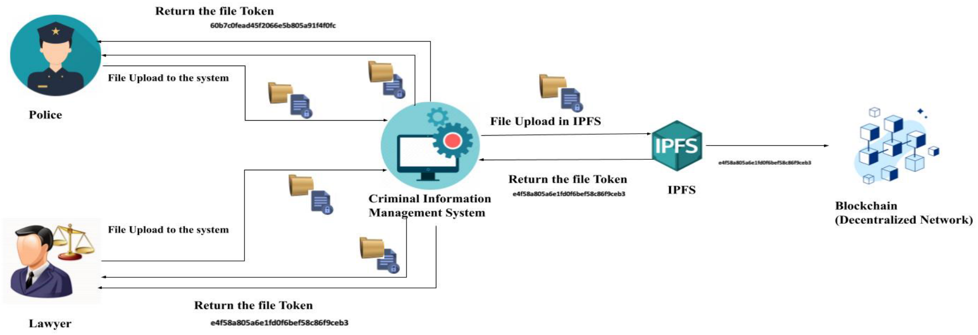

Return the file Token
60b7c0fead45f2066e5b805a91f4f0fc
File Upload to the system
Police
File Upload in IPFS
IPFS
e4f58a805a6e1fd0f6bef58c86f9ceb3
Return the file Token
e4f58a805a6e1fd0f6bef58c86f9ceb3
Criminal Information
Management System
Blockchain
(Decentralized Network)
File Upload to the system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

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:

1. 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.

2. 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.
3. 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.
4. 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.

Secure File Sharing Management System

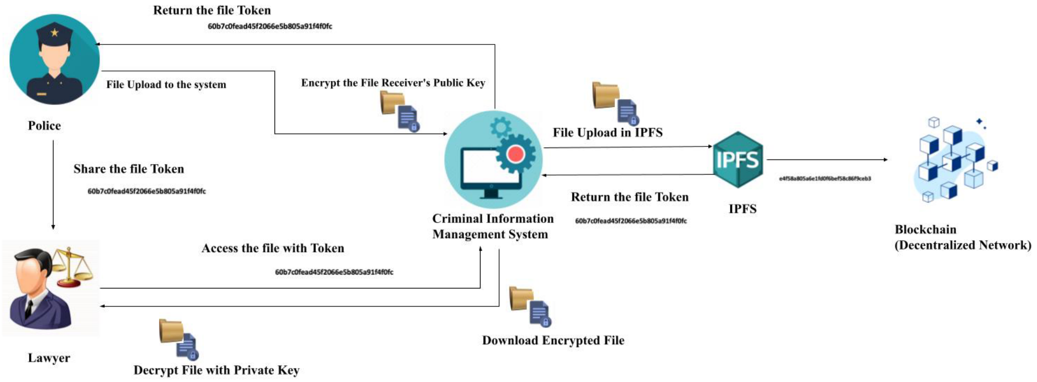

Return the file Token
60b7c0fead45f2066e5b805a91f4f0fc
Police
File Upload to the system
Encrypt the File Receiver's Public Key
File Upload in IPFS
IPFS
e4f58a805a6e1fd0f6bef58c86f9ceb3
Blockchain
(Decentralized Network)
Share the file Token
60b7c0fead45f2066e5b805a91f4f0fc
Return the file Token
60b7c0fead45f2066e5b805a91f4f0fc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

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:

1. 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.
2. 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.
3. 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.

4. 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.
5. 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.

Chain of Custody

The proposed system will have to consists of the following methodologies to achieve the goals of the research. This methodology provides a general framework for implementing a blockchain-based chain of custody evidence management system, but the specific steps and processes may vary depending on the organization's needs and the chosen blockchain platform. This method's primary phase is to derive concepts from knowledge base data and then apply the deductive process to create a relationship between the model's key variables. The overall procedure emphasizes a continuous dialogue between the phases of inductive data and analysis. Ultimately, this leads to the development of a sound analysis of the potential and applicability of blockchain and smart contracts to enhance Chain of Custody and the model for handling digital evidence. Additionally, fundamental metrics are taken into account to enhance traceability and evidence sources, such as evidence:

- Location of the data when generated.
- Type and format
- Time elapsed since stored.
- Current control and security measures
- Last accessibility and by who
- Last review
- The owner of data, who is responsible for the data.
- Transfer procedure

More than this, there are some additional methodologies listed here to develop out proposed system.

Identify the requirements: Define the system requirements based on the needs of the stakeholders and the goals of the organization.

Design the user interface: Create a user-friendly interface that allows authorized users to interact with the system and perform necessary actions, such as adding or retrieving evidence.

Integrate with existing systems: Integrate the blockchain-based chain of custody system with other relevant systems, such as forensic tools or case management software.

Train users: Train all relevant users, including investigators, administrators, and IT staff, on how to use the new system effectively and securely.

Test and deploy: Conduct thorough testing to ensure the system is functioning as expected and that the evidence is secure. Deploy the system and monitor its usage to identify any potential issues or improvements.

Maintain and update: Regularly maintain and update the system to ensure it remains secure and meets the changing needs of the organization.

The proposed system will have to consists of the following methodologies to achieve the goals of the research. This methodology provides a general framework for implementing a blockchain-based chain of custody evidence management system, but the specific steps and processes may vary depending on the organization's needs and the chosen blockchain platform. This method's primary phase is to derive concepts from knowledge base data and then apply the deductive process to create a relationship between the model's key variables. The overall procedure emphasizes a continuous dialogue between the phases of inductive data and analysis. Ultimately, this leads to the development of a sound analysis of the potential and applicability of blockchain and smart contracts to enhance Chain of Custody and the model for handling digital evidence. Additionally, fundamental metrics are taken into account to enhance traceability and evidence sources, such as evidence:

- Location of the data when generated.
- Type and format
- Time elapsed since stored.
- Current control and security measures
- Last accessibility and by who
- Last review
- The owner of data, who is responsible for the data.
- Transfer procedure

More than this, there are some additional methodologies listed here to develop out proposed system.

- **Identify the requirements**: Define the system requirements based on the needs of the stakeholders and the goals of the organization.
- **Design the user interface**: Create a user-friendly interface that allows authorized users to interact with the system and perform necessary actions, such as adding or retrieving evidence.
- **Integrate with existing systems**: Integrate the blockchain-based chain of custody system with other relevant systems, such as forensic tools or case management software.
- **Train users**: Train all relevant users, including investigators, administrators, and IT staff, on how to use the new system effectively and securely.
- **Test and deploy**: Conduct thorough testing to ensure the system is functioning as expected and that the evidence is secure. Deploy the system and monitor its usage to identify any potential issues or improvements.
- **Maintain and update**: Regularly maintain and update the system to ensure it remains secure and meets the changing needs of the organization.

2.2. Overall System Diagram

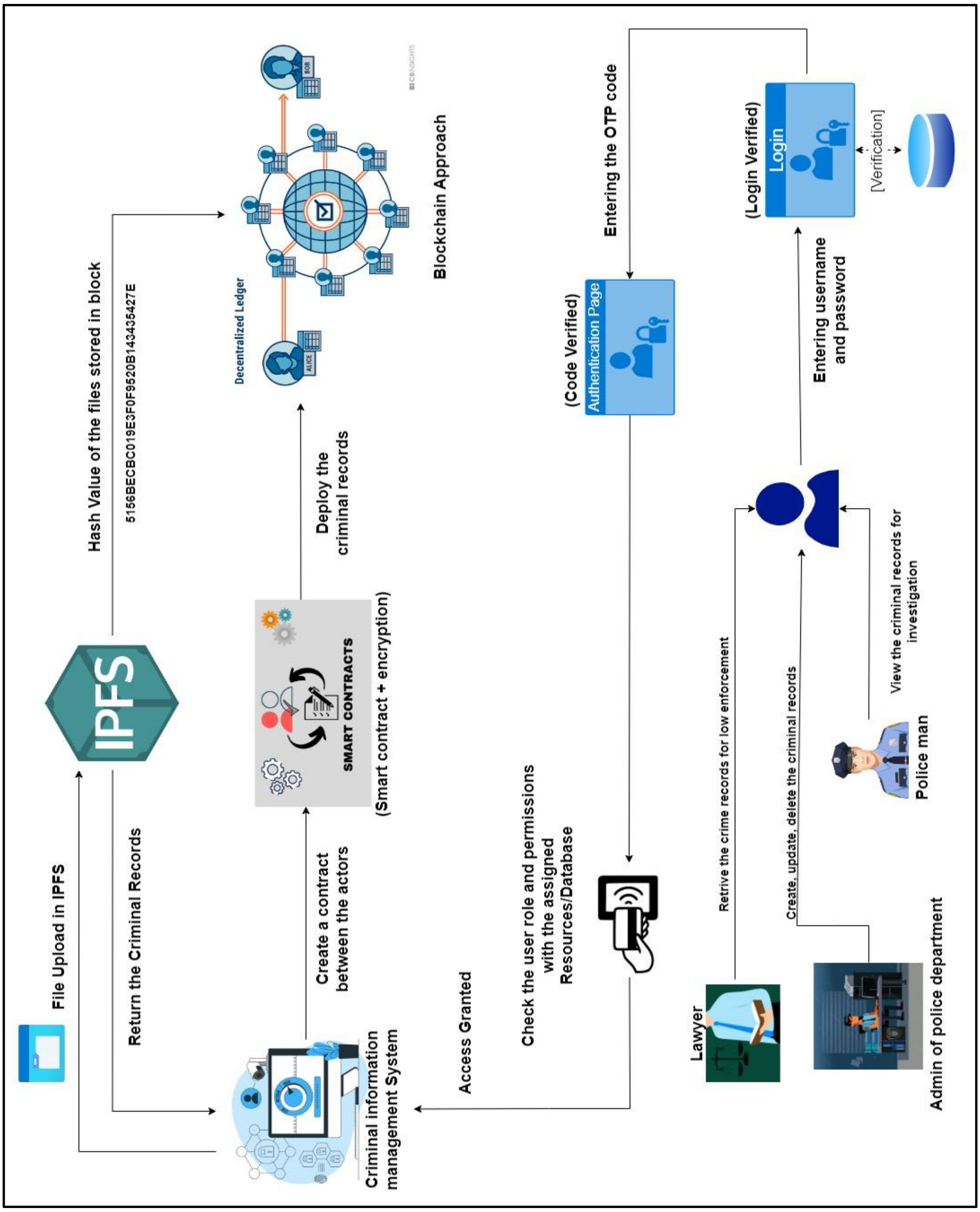

File Upload in IPFS
Return the Criminal Records
IPFS
Hash Value of the files stored in block
5156BECBC019E3F0F9520B143435427E
Decentralized Ledger
ALICE
BOB
CB INSIGHTS
Blockchain Approach
Create a contract between the actors
SMART CONTRACTS
(Smart contract + encryption)
Deploy the criminal records
Criminal information management System
Access Granted
Check the user role and permissions with the assigned Resources/Database
(Code Verified)
Authentication Page
Entering the OTP code
(Login Verified)
Login
[Verification]
Entering username and password
Retrive the crime records for low enforcement
Create, update, delete the criminal records
View the criminal records for investigation
Lawyer
Admin of police department
Police man

Figure 2.2. 1: Overall System Diagram

2.3. System Development Process

In the quest to design, develop, and implement a Blockchain-Based Criminal Information Management System (CIMS) for Sri Lanka, our research journey has been marked by a commitment to innovation and adaptability. At the heart of this endeavor lies the meticulous orchestration of the system development process, a journey guided by the principles of agility and responsiveness. In recognition of the dynamic and evolving landscape of criminal information management, we chose to adopt the Agile Software Development Methodology - a nimble and iterative approach that prioritizes collaboration, flexibility, and the continuous refinement of the system. Figure 2.3. 1, will provide an explanation of the development process.

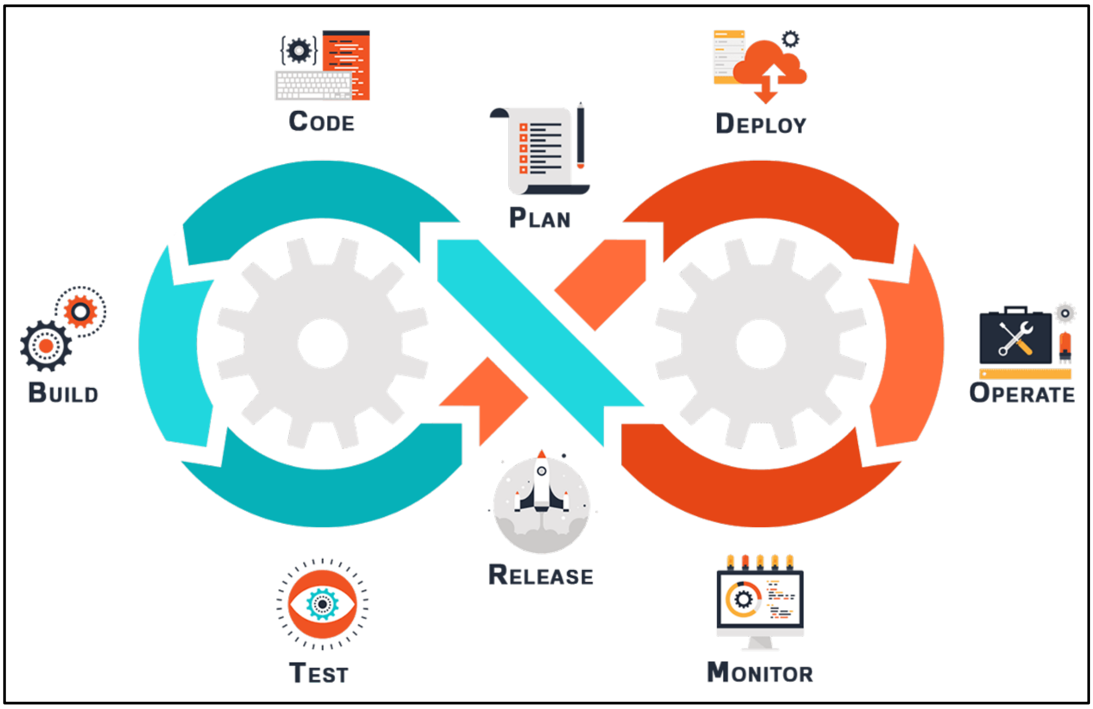


Figure 2.3. 1: Agile Software Development Methodology
Downloaded from PNGEGG [7]

2.3.1. A Framework for Innovation and Adaptation

The Agile Software Development Methodology, renowned for its versatility and iterative nature, has played a pivotal role in shaping the development of our blockchain-based CIMS. Unlike traditional, linear development approaches, Agile places a premium on close collaboration among cross-functional teams, frequent reassessment of project goals, and the seamless integration of feedback from end-users.

This methodology aligns harmoniously with the ever-changing dynamics of criminal information management, enabling us to respond swiftly to emerging requirements and challenges.

2.3.2. Iterative Progress: The Agile Advantage

Within the context of our research, the Agile approach has manifested as a series of iterative cycles, each designed to build upon the previous one. These iterations have enabled us to continuously refine our system, incorporating new features, addressing potential issues, and ensuring that the end product aligns seamlessly with the evolving needs of law enforcement agencies, the judiciary, and the citizens of Sri Lanka. By breaking down the development process into manageable increments, Agile has allowed us to strike a delicate balance between innovation and adaptability.

In the forthcoming sections, we delve into the specifics of our Agile-based system development process, providing insight into our collaborative workflows, user stories, and sprint cycles. We also explore the unique challenges and advantages that arose as a result of this methodology's application in the development of our blockchain-based CIMS, shedding light on how Agile principles fostered innovation and responsiveness throughout the journey.

Project managers adopted Scrum as a straightforward Agile development methodology to manage a range of iterative and incremental projects. Here, the product owner will create a product backlog using Scrum, and the development team will then find and rank system features in accordance [8].

2.4. Commercialization Plan

2.4.1. Targeted Audience

The Blockchain-Based Criminal Information Management System is a system that everyone within a country should have access to. Civilians will have the opportunity to report incidents and crimes that they have witnessed. The Blockchain-Based Criminal Information Management System will need to have different login privileges; for example, the privileges that a civilian should have is to report a crime, police officers should be able to report crimes, look into crime folders, investigate through the documentation, etc.

The authentication system that was proposed will be implemented no matter the login privilege the user has. Additionally, since this is an authentication system and can be implemented separately, this system can be used by other systems, applications, and software. So, if the targeted audience were listed for this authentication system, it would be as the following.

- Blockchain-Based Criminal Information Management System Users
    - Civilians
    - Law Enforcement
    - Police Officers
- Social Media Applications
- Hospitals
- Police Departments
- Vulnerability Scanning Tools
    - Example: Acunetix
- Cyber Security Monitoring Tools
    - Example: CrowdStrike

2.4.2. Advertising and Communication

Authentication systems are commonly used in every system and software, so promoting such systems would not be that hard. Since this proposed system will increase security to a greater level, vendors and service providers will want to use this system. A few of the methods to promote this system are;

- International Conferences
- Local Conferences
- Cold Calls
- Advertisements

In this scenario, the main advertising and communication method would be through International and Local Conferences.

3. IMPLEMENTATION & TESTING

In the realm of innovation and security, where computerized headways address the issues of the rule of law, a thrilling exertion is arising that could change how criminal data is dealt with. Picture this occurrence in the wonderful island country of Sri Lanka - it's tied in with making a better approach to oversee criminal data utilizing blockchain innovation. This isn't just about utilizing extravagant tech; it's tied in with ensuring data is really secure and mirroring the common craving for a more secure society.

For the implementation a considerable amount of time was spent, and it divirated us from the initial timeline; but with some of the minor extensions that were provided for the research, we were able to get back into track and with some additional hours into the implementations and developments.

After the initial configurations and implementations were completed, the system was tested to its core to see how it would act and handle the required load of power. Based on the Gantt Chart that is provided in the following section (3.1.1. Gantt Chart for the System Implementation), the testing of the system was taken into consideration in the third phase of the system development, and nearly a duration of two weeks were allocated for the system testing component by component.

Later on, after the entire system has been implemented and configured into one, there will be another testing conducted to see the overall functionalities and completion. The final testing is yet to happen in the fifth phase of the system development and implementation.

This fragment remains as a demonstration of development and ingenuity, where each line of code carves the story of progress and every security layer strengthens and discloses another layer of trust. The Confirmation Framework inside the Blockchain-Based Criminal Data The board Framework isn't simply a mechanical accomplishment; it is a recognition for the potential when aim and development meet.

3.1. System Implementations

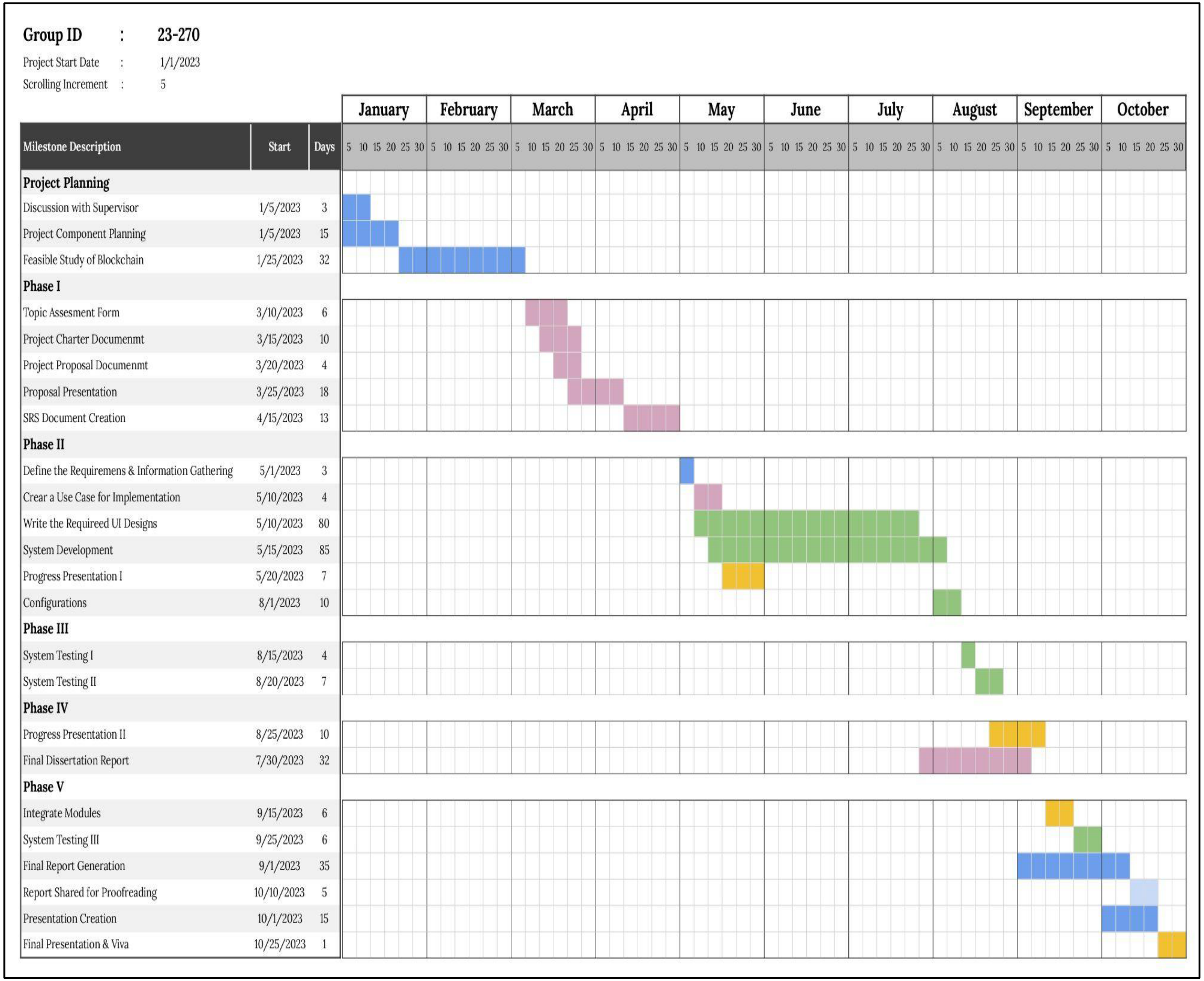
System implementations and documentations were planned for the entire year of 2023; there were some bottlenecks that were met during all these phases, but by the end of the required date, I was able to fully complete and present the finalized system with its all functionalities.

For the system implementations, technologies such as the following were used with the additional knowledge of blockchain, SQL, and vast areas of more;

- Ethereum
- Solidity
- React JS
- Ganache Personal Blockchain
- HTML
- CSS
- Java Script
- Python
- HMAC Algorithm
- Encryption
- Decryption
- InterPlanetary File System

Since there was a learning curve, it was beneficial for the success of the research and for our own knowledge, since most of the technologies that were in place had to be learned from scratch and develop the system in its entirety within the given short time duration. As a group we were able to discuss each of the required components and help out each other with our knowledge and expertise in each segment to make this research a success.

3.1.1. Gantt Chart for the System Implementation



Group ID : 23-270

Project Start Date : 1/1/2023

Scrolling Increment : 5

Milestone Description	Start	Days
Project Planning		
Discussion with Supervisor	1/5/2023	3
Project Component Planning	1/5/2023	15
Feasible Study of Blockchain	1/25/2023	32
Phase I		
Topic Assesment Form	3/10/2023	6
Project Charter Documenmt	3/15/2023	10
Project Proposal Documenmt	3/20/2023	4
Proposal Presentation	3/25/2023	18
SRS Document Creation	4/15/2023	13
Phase II		
Define the Requiremens & Information Gathering	5/1/2023	3
Crear a Use Case for Implementation	5/10/2023	4
Write the Requireed UI Designs	5/10/2023	80
System Development	5/15/2023	85
Progress Presentation I	5/20/2023	7
Configurations	8/1/2023	10
Phase III		
System Testing I	8/15/2023	4
System Testing II	8/20/2023	7
Phase IV		
Progress Presentation II	8/25/2023	10
Final Dissertation Report	7/30/2023	32
Phase V		
Integrate Modules	9/15/2023	6
System Testing III	9/25/2023	6
Final Report Generation	9/1/2023	35
Report Shared for Proofreading	10/10/2023	5
Presentation Creation	10/1/2023	15
Final Presentation & Viva	10/25/2023	1

Figure 3.1. 1: Gantt Chart for the System Implementation

3.2. System Testing

With the system implemented successfully, required testing was done to see how the system would function with actual data entered, with mistakes and errors that could happen in the day-to-day use. A table research was conducted to find what are the main points that needed to be focused during this testing and with the practical knowledge of using the system, those data and details were considered to conduct the required testing for the authentication system.

The key aspects and the implementations that were tested can be categorized into two different segments as;

- Interface Related Configurations
- Security Related Configurations

The following tables includes the key aspects and the implementation with the results or the status that was recorded during the testing period with comments.

	Test Date	Implementation	Status
Interface Related	08/15/2023	System Home Page	Successful
	08/15/2023	User Login Page	Successful
	08/15/2023	User Signup Page	Successful
	08/15/2023	Police Login Page	Successful
	08/15/2023	Admin Login Page	Successful
	08/15/2023	OTP Entering Page	Successful
	All the above-mentioned pages (system home page, user login page, user signup page, police login page, admin login page, and OTP entering pages) were tested thoroughly and all the design level and		

	activity level requirements are successfully implemented and working.		
	08/17/2023	User Dashboard	Successful
	08/17/2023	Police Dashboard	Successful
	08/17/2023	Admin Dashboard	Successful
	All the above-mentioned pages (user dashboard, police dashboard, and admin dashboard) were tested thoroughly. All data are being synced and displayed on dashboards as well as all the forms that are included are functioning as expected without any issues.		
	08/17/2023	Secure File Upload and Download Pages	Successful
	08/17/2023	Log management Interfaces	Successful
	08/17/2023	Criminal Record Upload Pages	Successful

Table 3.2. 1: Interface Related Testing

	Test Date	Implementation	Status
Security Related	08/15/2023	Username/Password Rules & Functional -ities	Successful
	During a user signup, the set rules are working as expected and it increases the security of the system. The set rules for the passwords that the users needs to use are as following; ● Passwords must be between 10 to 15 characters ● Password must contain at least one uppercase letter ● Password must contain at least one digit ● The password must contain at least one special character. All these rules and functionalities that were mentioned have been tested and they are working as expected without any bugs.		

<table>
<tr><td rowspan="10"></td><td>08/15/2023</td><td>Username/Password Authentication</td><td>Successful</td></tr>
<tr><td colspan="3">A configuration has been built into the system to provide a timeout when the user enters any incorrect username and password to the system.
● Max attempts: 5
● Lockout time: 300 seconds (5 minutes)
● Extend lockout time: 3600 seconds (60 minutes)
These configurations have been tested, and they are working as expected without any issues.</td></tr>
<tr><td>08/16/2023</td><td>OTP Code Rules & Functionalities</td><td>Successful</td></tr>
<tr><td colspan="3">For the OTP code generation, as per the main requirement the shift was made to improve the number of codes from 59,049 → 60,466,176.
This was tested and the OTP code is being generated successfully.</td></tr>
<tr><td>08/16/2023</td><td>OTP Code Authentication</td><td>Successful</td></tr>
<tr><td colspan="3">A 6-Character code will be generated and it should be entered to authenticate the user and to move forward the user to the system. A timeout is set within 60 seconds, by giving plenty of time for the users to enter the authentication code. Without the authentication being successful, the user cannot move to the next page.</td></tr>
<tr><td>08/16/2023</td><td>Email Verification</td><td>Successful</td></tr>
<tr><td colspan="3">With the OTP 6-Character code being generated successfully, the code is passed to the email; this requires reading the database files and identifying the user by their username, and with that identify the email address of that user and pass the OTP code to that address.</td></tr>
<tr><td>08/17/2023</td><td>Checking whether uploaded and downloaded file Hash Values are the same</td><td>Successful</td></tr>
</table>

	08/17/2023	Logs are recorded correctly	Successful
	08/17/2023	Data entering for the blockchain	Successful
	08/17/2023	Data retrieving from the blockchain	Successful

Table 3.2. 2: Security Related Testing

4. RESULTS & DISCUSSION

4.1. Results of the System

The software solution designed for the Blockchain-based criminal information management system requires comprehensive evaluation by a range of stakeholders, including developers, testers, and potential users. In the initial stages of our research, it became evident that establishing trustworthiness was a fundamental requirement. However, the precise definition and understanding of trust within the context of information solutions were not well- defined.

The emergence of blockchain technology has presented a promising avenue for addressing this trust deficit. Globally, there is a growing body of research exploring the concepts of trust and privacy within blockchain-based systems. While these concepts have gained traction in academic and research circles, they have yet to achieve widespread recognition among the public, particularly within the Sri Lankan context.

The concept of cryptocurrency or virtual currency, which is closely tied to blockchain technology, has gained acceptance in many countries. In Sri Lanka, there is a burgeoning interest in virtual currencies, especially among the younger population. However, it is important to note that the lack of endorsement by the Sri Lankan Central Bank has posed a challenge to fostering trust in blockchain-based solutions within the country.

These considerations underscore the need for rigorous evaluation, education, and awareness- building efforts when implementing a blockchain-based criminal information management system in Sri Lanka. Building trust and confidence in the technology among stakeholders, including potential donors, is pivotal to the successful adoption of such innovative solutions

Results

Software testing

The testing and evaluation process for the proposed Blockchain-based criminal information management system is structured around predefined use cases derived from the initial requirement gathering phase. These use cases encompass critical functionalities such as initiating a criminal information request, validating the request (both positive and negative outcomes), approving donations, and updating donor information. To effectively evaluate the system, a set of well-defined test cases has been established. These test cases are specifically designed to assess the identified features outlined in the solution. Below are some notable test cases:

Entity Registration: This initial set of test cases focuses on registering system entities, including law enforcement agencies, individuals involved in criminal cases, and authorized users. The successful execution of these test cases demonstrates the system's functionality and its ability to handle entity registration effectively.

Data Integrity and Usability: The system undergoes extensive testing with sample data to ensure data integrity and usability. The goal is to evaluate the suitability of blockchain technology in preserving the integrity of criminal information and its usability for the application's users.

Authentication and Authorization: Test cases are devised to evaluate the authentication and authorization mechanisms within the system. This ensures that only authorized users can access and modify criminal information, thereby enhancing security and data confidentiality.

Criminal Information Requests: The testing process involves simulating criminal information requests and assessing the system's responsiveness in handling such requests. It evaluates whether the system can efficiently process and validate criminal information requests.

Functional Validation: Throughout the testing phase, the system's functionality is continuously validated to ensure that it consistently performs as expected. This includes confirming that the system meets the predefined use cases and requirements.

Performance Assessment: Performance testing is conducted to evaluate the system's responsiveness, scalability, and overall performance under various loads and conditions.

Data Security: The security of criminal information stored on the blockchain is a paramount concern. Test cases are designed to assess data security measures and confirm that sensitive information remains protected from unauthorized access.

The development testing phase primarily focuses on aligning the system with the identified requirements. Sample data is used for testing, and the system's usability is assessed in the context of criminal information management.

4.2. Final Discussions

As we plunge into the last leg of our investigation, now is the ideal time to have a smart discussion about what we have uncovered. This is where we make a stride back, set up the pieces, and figure out the excursion we've been on. We have discussed results and tests, yet presently it's tied in with looking past the surface and understanding what everything implies.

During the segment of 'System Overview', we have discussed the in depth overview of the Blockchain-Based Criminal Information Management System In Sri Lanka and how it should work; and when we moved into the segment of '2.2.Overall System Diagram', we saw the system diagrams and how each component contributes to the development of the overall system and its security. During the segment of '2.3. System Development Process' we have mentioned the development process that was used to implement and develop the Blockchain-Based Criminal Information Management System for the citizens of Sri Lanka.

During the segment of 'System Implementations', we discussed how the system was implemented, what technologies were used, about the timelines of the Blockchain-Based Criminal Information Management System throughout the year (Gantt Charts). Moving to the segment of 'System Testing', we dug deep into the system and verified that every webpage, functionalities and security implementations are working without any bugs or introptions.

As a final step, a final system test was conducted to see the system funutilities in play with real end users to see how effective this provided Blockchain-Based Criminal Information Management System would be and how efficient this system performs. With the results that were gathered and discussed during the segment of '4.1. Results of the System', it is safe to say that the beta test was successful and the system implementations and configurations are as expected.

If I were to sum up everything about the implementations of the Blockchain-Based Criminal Information Management System, it would be that the newly proposed and implemented Blockchain-Based Criminal Information Management System was a success.

Smart Contract Testing – Remix IDE

Remix IDE stands as an open-source web application designed to facilitate the development, deployment, and testing of smart contracts on the Ethereum blockchain. It offers an integrated graphical user interface (GUI) that enhances the efficiency and clarity of the testing and learning process for developers. Within Remix IDE, developers can seamlessly write, compile, and deploy smart contracts. Subsequently, they can interact with these contracts by providing the required inputs to the blockchain through the smart contract functions and retrieving information using the same methods. Figure 4.1 provides an illustrative representation of the smart contract testing process within Remix IDE. The assessment of blockchain functionality can be quantified by measuring the gas consumption associated with each transaction and its impact on the Ether (ETH) balance of individual blockchain user accounts. Notably, actions such as recording data on the blockchain incur gas costs, whereas reading information from the blockchain is gas-free. Furthermore, the Ganache personal blockchain offers valuable insights into each user account's coin balance and transaction- related details. It provides a comprehensive overview of transaction history and associated information.

5. CONCLUSION

Criminal information management has long grappled with issues of integrity, fraud, and an uneven distribution of resources. Traditional methods of managing criminal data have relied on manual processes or centralized systems, which have often been susceptible to fraudulent activities, scams, and a lack of transparency. The emergence of blockchain technology has introduced a promising paradigm shift, offering attributes such as immutability, decentralized public ledgers, consensus mechanisms, unanimous decision-making, and smart contract automation. These features make blockchain an ideal candidate for enhancing the management of criminal information.

Extensive research, as highlighted in the literature review, has explored the application of blockchain in the realm of criminal information management, particularly in the domains of funding and resource allocation. Notably, blockchain's utility has expanded beyond financial transactions to encompass areas like blood and organ donations, as indicated by the literature survey. However, one critical aspect that has not received sufficient attention is the validation of criminal information requests for authenticity and the establishment of trust through immutability.

The validation of requests has been rigorously examined in specific contexts, such as student degree verification processes, where blockchain has demonstrated its effectiveness. Therefore, this research proposes the integration of a blockchain-based solution to validate criminal information requests. By upholding transparency, this approach allows donors to witness firsthand how their contributions are channeled towards fulfilling these requests. Blockchain technology's core principles, including transparency and the elimination of intermediaries, can be harnessed to instill trust and authenticity in the validation of criminal information requests.

The implementation of digital signatures emerges as a crucial component in this context, serving to validate the authenticity of users' requests and further fortify the trustworthiness of the criminal information management system. This is a criminal system based on the Sri Lanka police departments according to the GDPR and HIPAA. We addressed the existing problems with our proposed Blockchain technology.

Future Work

The prospects of blockchain technology hold immense promise on a global scale, with a significant focus on the domain of cybersecurity. While the blockchain ledger itself is public and distributed, its inherent security mechanisms ensure the safeguarding and verification of data. Employing advanced cryptography techniques, blockchain effectively mitigates vulnerabilities like unauthorized data manipulation. This robust concept of blockchain has the potential to revolutionize data management, particularly within government agencies. Its implementation can transform traditional data handling into an efficient and streamlined process, enhancing the overall performance and effectiveness of these institutions. Furthermore, blockchain's decentralized security features offer a heightened level of protection for cloud storage, significantly reducing susceptibility to hacking, data loss, or human errors when compared to centralized server-based storage.

In addition to its impact on cybersecurity, blockchain technology presents substantial opportunities within the healthcare sector. The healthcare industry in India, like many others, grapples with the challenge of insufficient data and time-consuming data compilation. Blockchain offers a solution by enabling the storage and real-time updating of crucial patient information, such as blood pressure and sugar levels, with the support of IoT devices and wearables. This transformative approach not only expedites data collection but also empowers healthcare professionals to monitor high-risk patients around the clock. In case of emergencies, blockchain facilitates instant alerts to caregivers and relatives, ensuring prompt intervention and support.

6. REFERENCES

[1] "Definition and Types of Information," 02 March 2022. [Online]. Available: https://www.lisedunetwork.com/definition-and-types-of-information/. [Accessed 18 March 2023].

[2] I. E. Team, "What Is Information Management? Definition and Benefits," Indeed, 11 March 2023. [Online]. Available: https://www.indeed.com/career -advice/career-development/what-is-information-management. [Accessed 18 March 2023].

[3] G. Skandha, "Rising crime wave amidst crises," June 2022. [Online]. Available: https://www.themorning.lk/articles/206633. [Accessed 18 March 2023].

[4] "GLOBAL ORGANIZED CRIME INDEX SRI LANKA," GLOBAL ORGANIZED CRIME INDEX. Available: https://ocindex.net/country/sri_lanka. [Accessed 18 March 2023].

[5] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?" in IT Professional, vol. 19, no. 4, pp. 68-72, 2017, doi: 10.1109/MITP.2017.3051335.

[6] A. Jain, S. Das, A. Singh Kushwah, T. Rajora and S. Saboo, "Blockchain-Based Criminal Record Database Management," 2021 Asian Conference on Innovation in Technology (ASIANCON), PUNE, India, 2021, pp. 1-5, doi: 10.1109/ASIANCON51346.2021.9544655.

[7] "Application Lifecycle Management," PNGEGG, [Online]. Available: https://www. pngegg.com/en/png-wttdj. [Accessed 22 March 2023].

[8] K. Brush and V. Silverthorne, "Agile software development," TechTarget, November 2022. [Online]. Available: https://www.techtarget.com/search softwarequality/definition/agile-software-development. [Accessed 22 March 2023].

[9] “Charity and Disaster Fraud”, FBI.org, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/charity-and- disaster- fraud (accessed Apr. 15, 2022)

[10] Singh, R. Rajak, H. Mistry and P. Raut, "Aid, Charity and Donation Tracking System Using Blockchain," *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, 2020, pp. 457-462, doi: 10.1109/ICOEI48184.2020.9143001.

[11] J. Lee, A. Seo, Y. Kim, and J. Jeong, “Blockchain-Based One-Off Address System to Guarantee Transparency and Privacy for a Sustainable Donation Environment,” *Sustainability*, vol. 10, no. 12, p. 4422, Nov. 2018 [Online]. Available: http://dx.doi.org/10.3390/su10124422

[12] .N. Bozic, G. Pujolle and S. Secci, "A tutorial on blockchain and applications to secure network control-planes," *2016 3rd Smart Cloud Networks & Systems (SCNS)*, 2016, pp. 1-8, doi: 10.1109/SCNS.2016.7870552.

[13] Jingyu Zhang, Siqi Zhong, Tian Wang, Han-Chieh Chao, Jin Wang, "Blockchain-based Systems and Applications: A Survey," *Journal of Internet Technology*, vol. 21, no. 1 , pp. 1- 14, Jan. 2020.

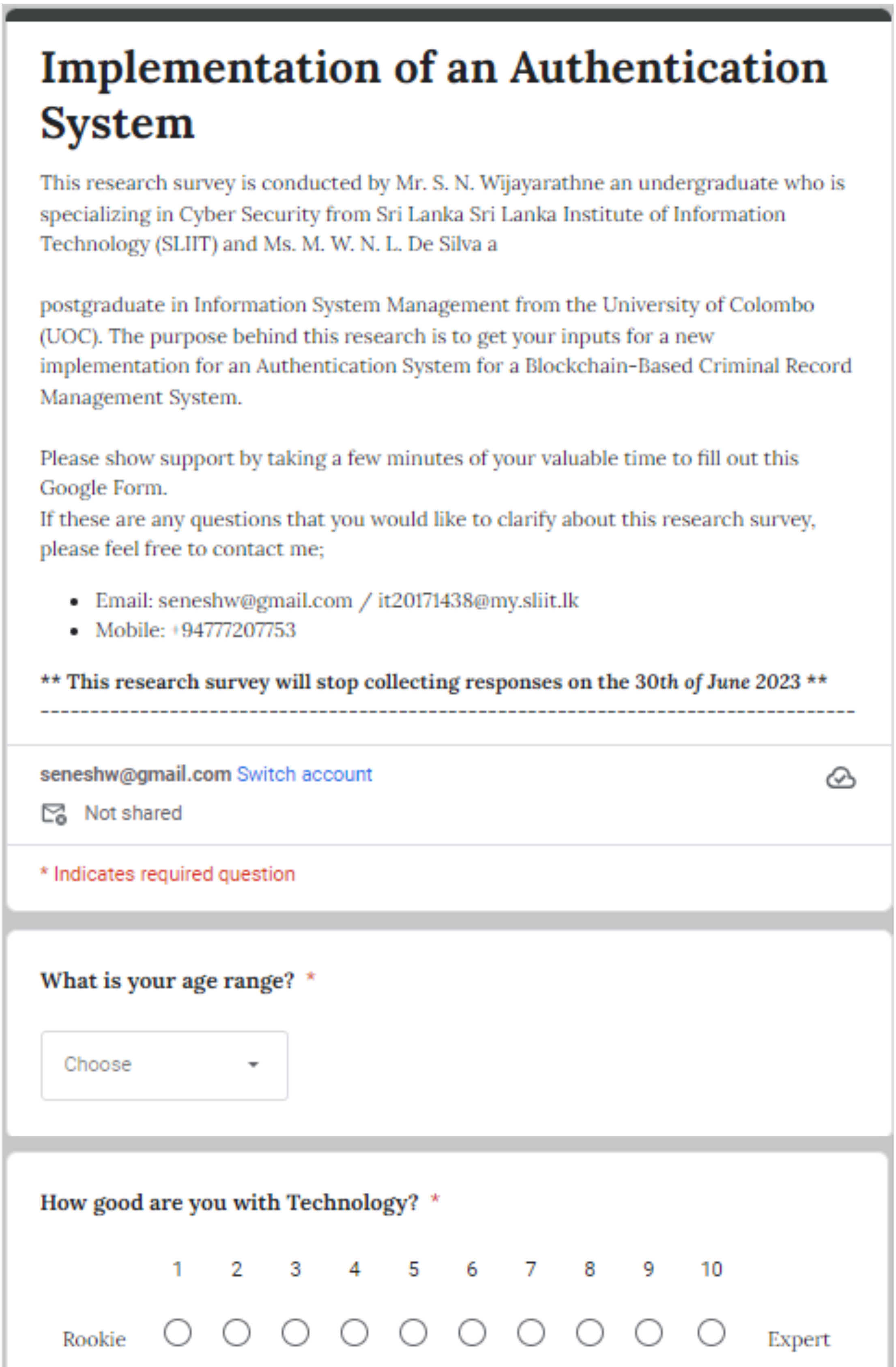
[14] .J. Garon, “*Legal Implications of a Ubiquitous Metaverse and a Web3 Future*.” https://ssrn.com/abstract=4002551),doi: http://dx.doi.org/10.2139/ssrn.4002551

[15] .“Introduction to Web3” ethereum.org. https://ethereum.org/en/web3/ (accessed Jul. 25, 2022).

[16] .k. Ashford, "What Is Bitcoin And How Does It Work?", forbes.com, https://www.forbes.com/advisor/investing/cryptocurrency/what-is-bitcoin (accessed June 13, 2021).

7. APPENDICES

Appendices A: Implementation of an Authentication System



Implementation of an Authentication System

This research survey is conducted by Mr. S. N. Wijayarathne an undergraduate who is specializing in Cyber Security from Sri Lanka Sri Lanka Institute of Information Technology (SLIIT) and Ms. M. W. N. L. De Silva a

postgraduate in Information System Management from the University of Colombo (UOC). The purpose behind this research is to get your inputs for a new implementation for an Authentication System for a Blockchain-Based Criminal Record Management System.

Please show support by taking a few minutes of your valuable time to fill out this Google Form.
If these are any questions that you would like to clarify about this research survey, please feel free to contact me;

- Email: seneshw@gmail.com / it20171438@my.sliit.lk
- Mobile: +94777207753

**** This research survey will stop collecting responses on the 30th *of June* 2023 ****
----

seneshw@gmail.com Switch account

Not shared

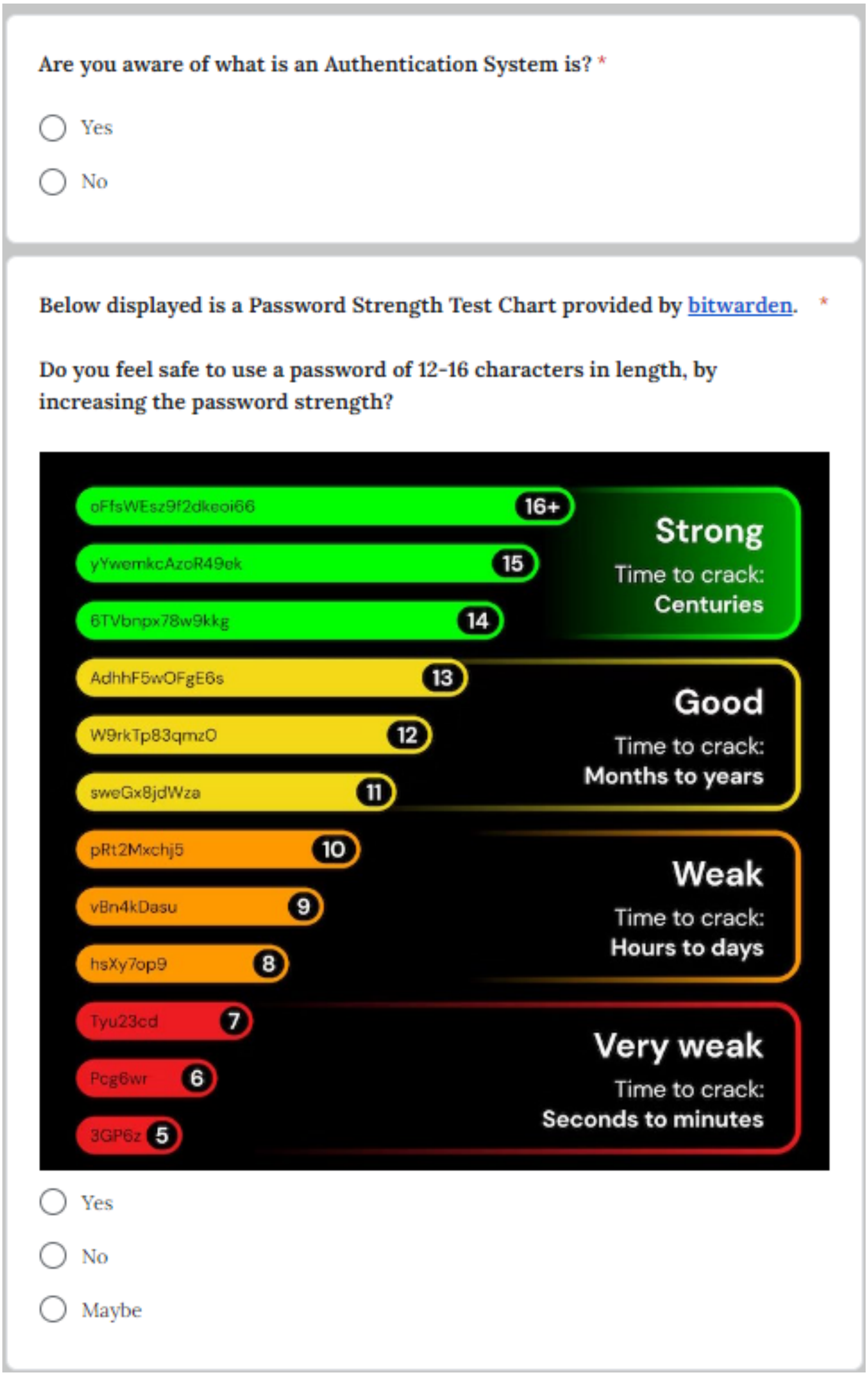
* Indicates required question

What is your age range? *

Choose ▾

How good are you with Technology? *

	1	2	3	4	5	6	7	8	9	10	
Rookie	○	○	○	○	○	○	○	○	○	○	Expert



Are you aware of what is an Authentication System is? *

○ Yes

○ No

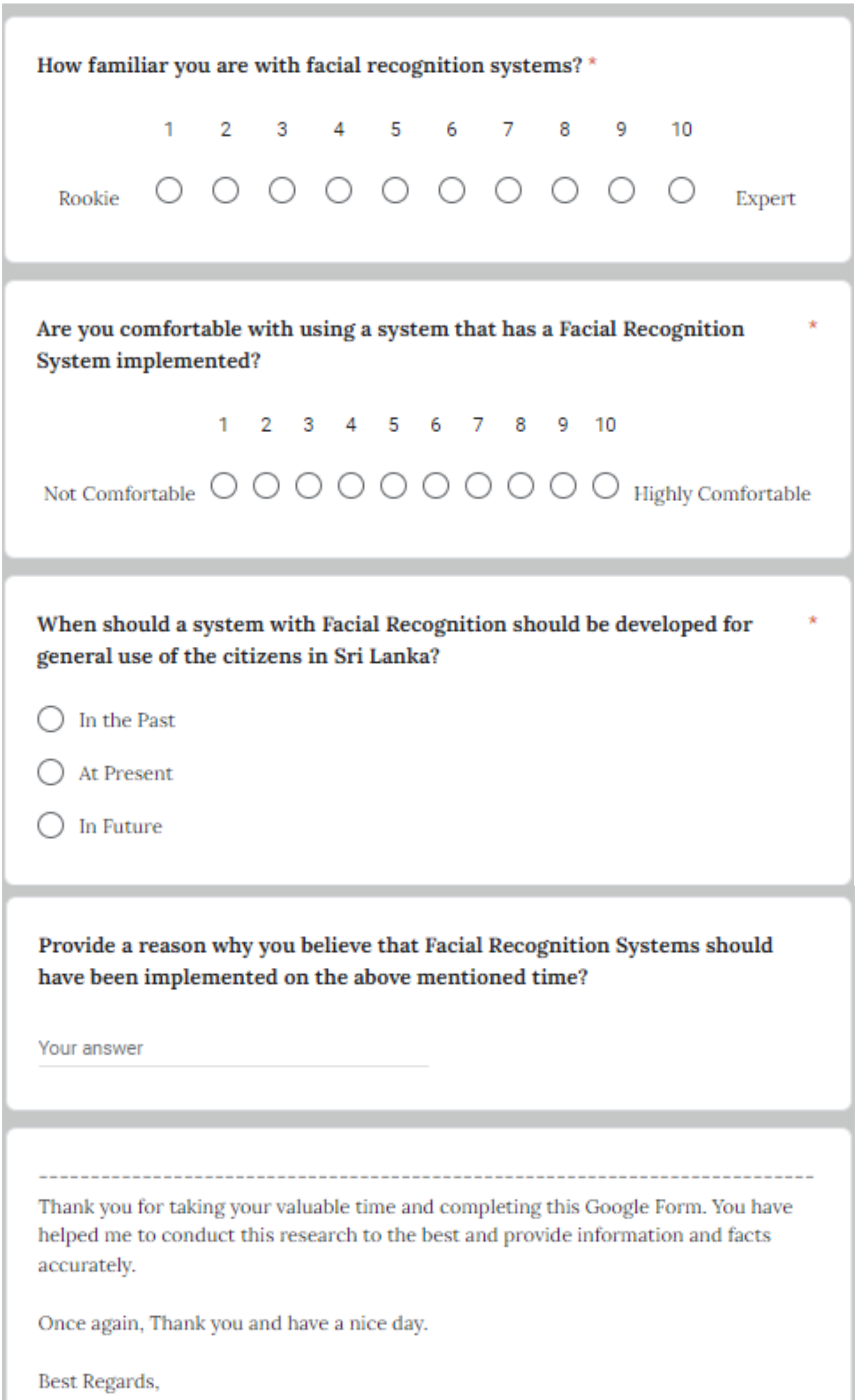
Below displayed is a Password Strength Test Chart provided by bitwarden. *

Do you feel safe to use a password of 12-16 characters in length, by increasing the password strength?

○ Yes

○ No

○ Maybe



How familiar you are with facial recognition systems? *

	1	2	3	4	5	6	7	8	9	10	
Rookie	○	○	○	○	○	○	○	○	○	○	Expert

Are you comfortable with using a system that has a Facial Recognition System implemented? *

	1	2	3	4	5	6	7	8	9	10	
Not Comfortable	○	○	○	○	○	○	○	○	○	○	Highly Comfortable

When should a system with Facial Recognition should be developed for general use of the citizens in Sri Lanka? *

○ In the Past

○ At Present

○ In Future

Provide a reason why you believe that Facial Recognition Systems should have been implemented on the above mentioned time?

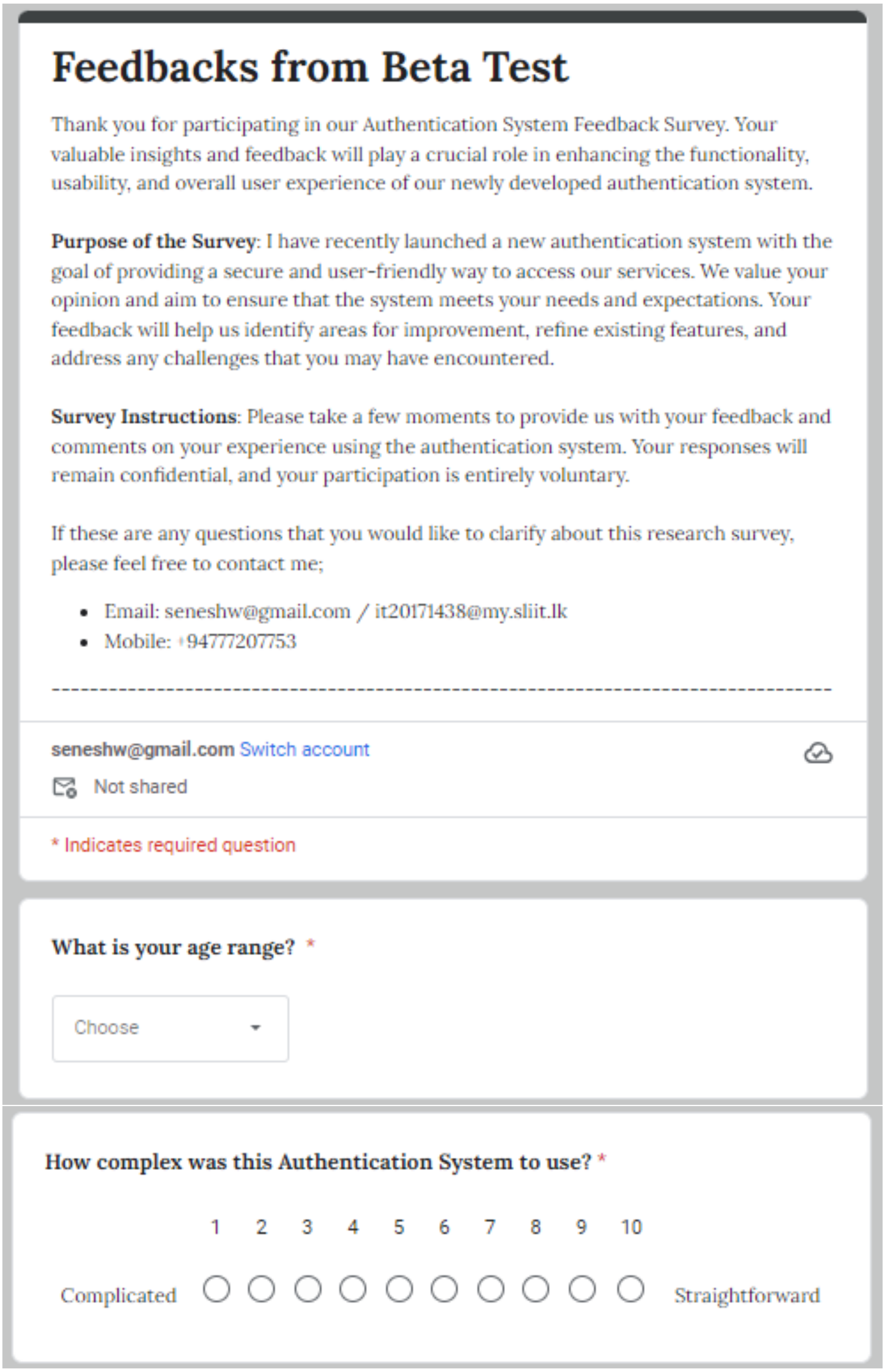
Your answer

Thank you for taking your valuable time and completing this Google Form. You have helped me to conduct this research to the best and provide information and facts accurately.

Once again, Thank you and have a nice day.

Best Regards,

Appendices B: Feedbacks from ‘Beta Test’



Feedbacks from Beta Test

Thank you for participating in our Authentication System Feedback Survey. Your valuable insights and feedback will play a crucial role in enhancing the functionality, usability, and overall user experience of our newly developed authentication system.

Purpose of the Survey: I have recently launched a new authentication system with the goal of providing a secure and user-friendly way to access our services. We value your opinion and aim to ensure that the system meets your needs and expectations. Your feedback will help us identify areas for improvement, refine existing features, and address any challenges that you may have encountered.

Survey Instructions: Please take a few moments to provide us with your feedback and comments on your experience using the authentication system. Your responses will remain confidential, and your participation is entirely voluntary.

If these are any questions that you would like to clarify about this research survey, please feel free to contact me;

- Email: seneshw@gmail.com / it20171438@my.sliit.lk
- Mobile: +94777207753

----

seneshw@gmail.com Switch account

Not shared

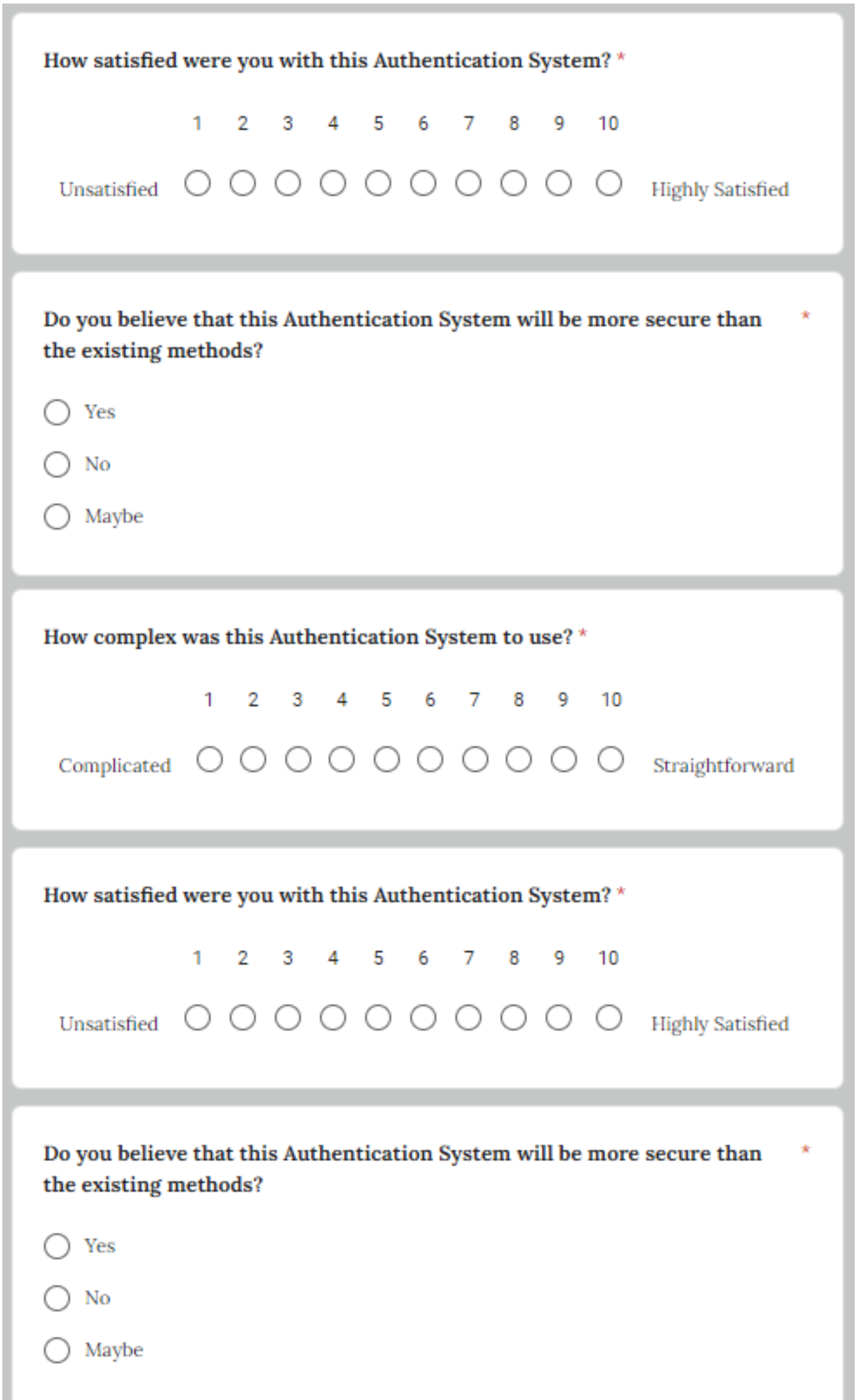
* Indicates required question

What is your age range? *

Choose ▾

How complex was this Authentication System to use? *

	1	2	3	4	5	6	7	8	9	10	
Complicated	○	○	○	○	○	○	○	○	○	○	Straightforward



How satisfied were you with this Authentication System? *

	1	2	3	4	5	6	7	8	9	10	
Unsatisfied	○	○	○	○	○	○	○	○	○	○	Highly Satisfied

Do you believe that this Authentication System will be more secure than the existing methods? *

○ Yes

○ No

○ Maybe

How complex was this Authentication System to use? *

	1	2	3	4	5	6	7	8	9	10	
Complicated	○	○	○	○	○	○	○	○	○	○	Straightforward

How satisfied were you with this Authentication System? *

	1	2	3	4	5	6	7	8	9	10	
Unsatisfied	○	○	○	○	○	○	○	○	○	○	Highly Satisfied

Do you believe that this Authentication System will be more secure than the existing methods? *

○ Yes

○ No

○ Maybe