BLOCKCHAIN-BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA

TMP-22-270

Project Proposal Report

Wijayarathne S. N – IT20171438

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

March 2023

BLOCKCHAIN-BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA

TMP-22-270

Project Proposal Report

Wijayarathne S. N – IT20171438

Supervisor: Mr. Kanishka Yapa

Co-Supervisor: Ms. Dinithi Pandithage

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

March 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**
Wijayarathne S. N	**IT20171438**	

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 can be 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

I 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, I would like to express my gratitude to my friends and family members for showing me all the support and advice for the individual component that I have selected. With their input and suggestions, I was able to look into various different paths.

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

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,

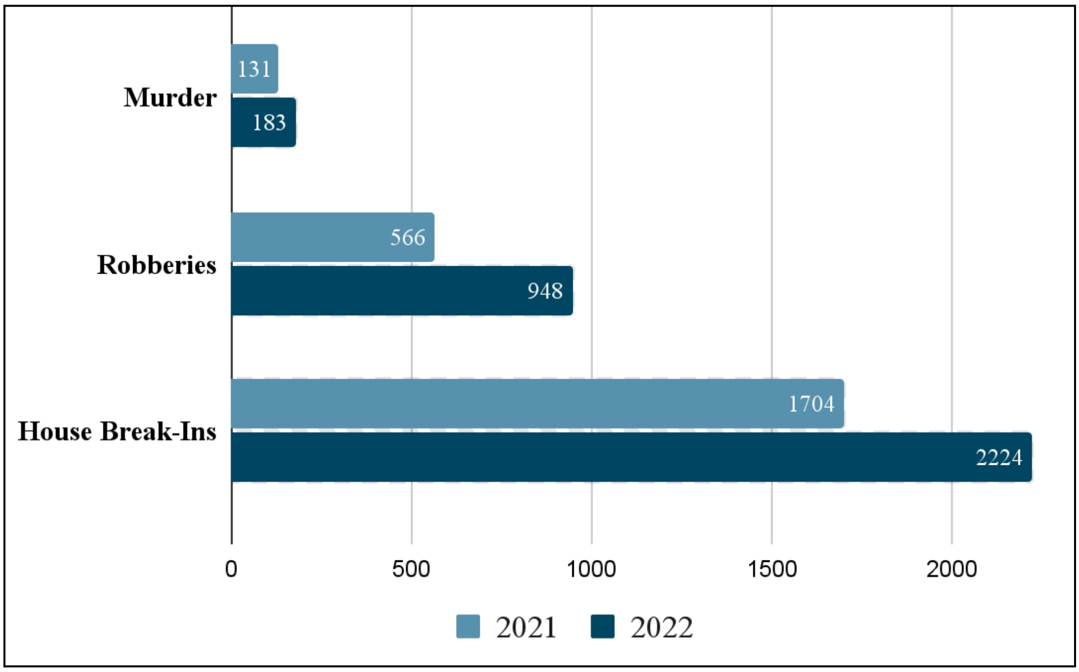

Figure 1.1. 1: Reported crimes in the first four months of 2021 and 2022

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.

The focus of this proposal is on; *Implementing a Multi-Factor Authentication system for the Blockchain-based Criminal Information Management System.* The most common authentication is two-factor authentication, also known as 2FA. This individual research started with an investigation into two-factor authentication (2FA). Two-Factor Authentication (2FA) is a widely used security measure that requires users to provide two different authentication factors to access their accounts, such as a password and a code sent to their mobile device.

2. RESEARCH PROBLEM

Research conducted by Emin Huseynov from the Sapienza University of Rome and Jean-Marc Seigneur from the University of Geneva has published a classic two-factor authentication flow chart and figure 1.3. 1 shows that [7];

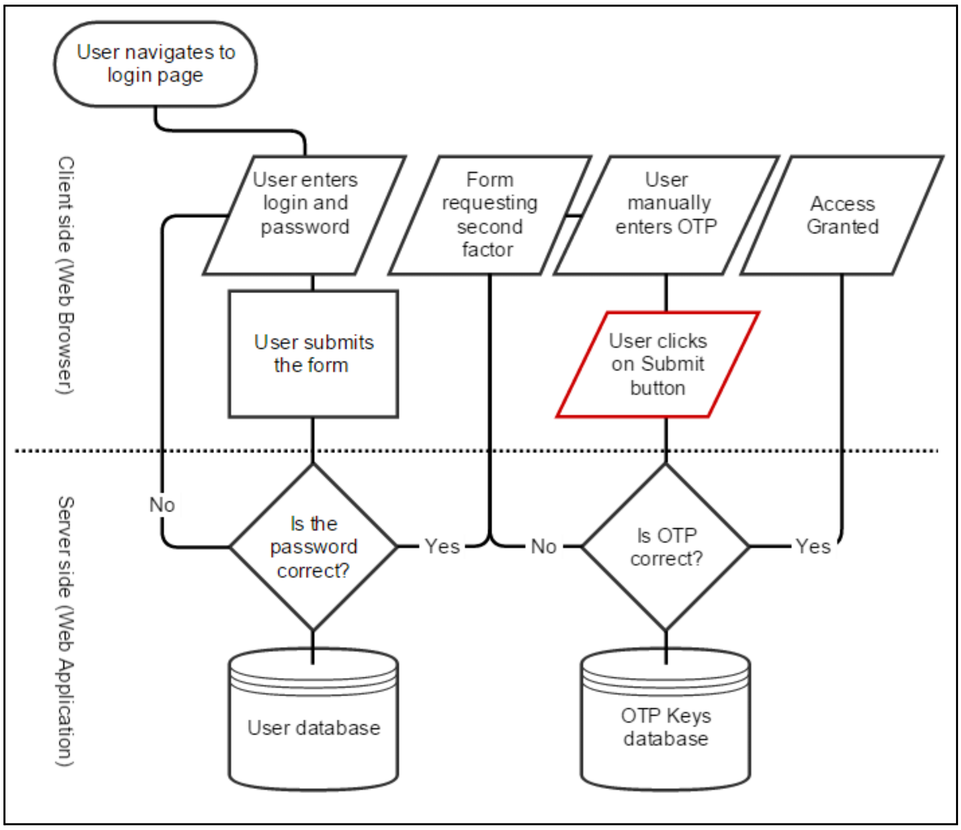
User navigates to login page
Client side (Web Browser)
User enters login and password
Form requesting second factor
User manually enters OTP
Access Granted
User submits the form
User clicks on Submit button
Server side (Web Application)
No
Is the password correct?
Yes
No
Is OTP correct?
Yes
User database
OTP Keys database

Figure 1.3. 1: Classic Two-Factor Authentication Flow Chart

However, like any security measure, 2FA needs to be more foolproof. Simple but effective methods can be taken to bypassing two-factor authentication and exploiting the required information to exploit two-factor authentication. Below mentioned are a few methods of two-factor authentication that can be exploited or bypassed:

- SIM Swapping
- Social Engineering
- Malware
- Man-in-the-middle
- Authentication app compromise
- Hardware token compromise

By these provided methods, 2FA can be exploited or bypassed, it can be done directly or indirectly. How the malicious actors can perform these exploits are listed in table 1.3. 1.

Type	**Description**
SIM Swapping	Aims to transfer a victim's phone number to a new SIM card controlled by the attacker. They can use it to intercept 2FA codes sent via SMS to the victim's phone if they have access.
Social Engineering	Requires the victim to reveal their 2FA code. This can be accomplished through methods like phishing emails or phone conversations in which the attacker pretends to be a real company and requests the code as part of a security check.
Malware	Malware can be used to intercept the generated 2FA code from the user's device or applications.
Man-in-the-middle	By intercepting the communication between the user and the server, attackers can steal the required 2FA codes from the user.
Authentication App Compromise	Authentication applications have vulnerabilities, and if an attacker manages to exploit it or gain access to a user's authentication app, the attacker can generate the required 2FA codes and use them as they please.
Hardware Token Compromise	Some 2FA systems require hardware tokens as the 2FA code, but if an attacker gains access to the hardware device, the attacker clones the device, or if the attacker exploits any vulnerability of the hardware device itself, the 2FA code will be exposed. Attackers can take advantage of the signature or the heat generated by the device to exploit its internal vulnerabilities.

Table 1.3. 1: Types and Description of how to bypass or exploit 2FA

As a Solution for two-factor authentication, multi-factor authentication (MFA) was developed. There are three common authentication factors when it comes to multi-factor authentication, and those factors would be [8];

- Knowledge Factor
  - Revealing information that no one knows to prove their identity is known as the knowledge factor. The most common questions would be; the name of their first pet, their mother's maiden name, the name of the street they lived in, etc. [8].
- Possession Factor
  - Uniquely owning something that can identify the user can be known as a possession factor. Mobile phones, security tokens, email accounts, and authenticator applications are just a few to name [8].
- Inherence Factor
  - Factors that the user inherence uses as an authentication method is what the inherence factor means. A few of the inherence factors are the user’s fingerprint, voice, eyes, face, and behavior [8].

With the advancement of technology, vulnerabilities and methods of bypassing multi-factor authentication (MFA) were identified. Technology advanced, computation power increased, and hackers became smarter. Table 1.3. 2 will show how a hacker can exploit or gather the required information for multi-factor authentication [8].

Factor	**Method**
Knowledge	Using information that only the user knows to move forward is a knowledge factor. With the improvement of technology and social media, hackers do not have to work hard as they used to work to gather information about someone over the internet since the user themselves would have uploaded or posted details about them. For example, people tend to post images of their pets with their names, tag the location of their homes, and mention their loved ones on social media. Just by going through the user's accounts, the details to exploit a knowledge factor can be

	collected. There are more hands-on methods as well for a hacker, such as phishing and social engineering [8].
Possession	Ownership of something that is unique to the user is required to move forward in the authentication process; this method is known as the possession method. The main downside of the possession factor is the risk of losing the unique items that can identify the users. Users can lose their mobile devices, hardware devices, email account passwords, etc. Misplacing these items or accounts can lead to the hacker retrieving the details that are needed. There are other methods that hackers can gain access to these devices, such as SIM cloning, exploiting vulnerabilities in the code level and the hardware level to gain system access, and brute-forcing/social engineering methods to hack into user email accounts, which are just a few methods [8].
Inherence	Factors the user inheritance from birth that is used for authentication can be known as the Inherence Factor. Out of all the mentioned factors, the inherent factor is considered to be the most secure. But with the enhancement of technology, individuals and hackers have identified/built devices to detect Inherence factors and control them as the hackers would please. There are numerous other ways that hackers can get hold of the required factors through indirect methods, such as dusting up the fingerprint from a glass mug and recording the user's voice through audio recorders, and with the advancement of Technology and Artificial Intelligence (AI), there are tools that can generate an individual face to live looking way just by uploading several pictures of that individual [8].

Table 1.3. 2: Types and Description of how to bypass or exploit MFA

If we consider the details that are mentioned in the above table (table 1.3. 2), that makes us question whether 2FA or MFA is secure. There are much better and more advanced security methods and authentication methods, but they are not for day-to-day use, and they will cost a fortune. Inherence factors are also mainly used in industries since the general human would not purchase machines and devices that would cost them a lot to implement and maintain.

3. RESEARCH OBJECTIVES

3.1. Main Objective

'*Blockchain-based criminal information management system in Sri Lanka*' this topic is selected with four sub-components, and those four sub-components are;

- Implementing smart contracts between criminal information management systems and blockchain technology.
- Implementing a Multi-Factor authentication (MFA) 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 the decentralized network.

The focus of this proposal is based on '*Implementing Multi-Factor Authentication (MFA) system for the Blockchain-Based Criminal Information Management System*'. The main objective of this sub-objective would be to ensure high security for the users who are entering the Blockchain-Based Criminal Information Management System to enter, delete, modify, or read gathered data. Criminal Information should be managed carefully since misplacing these records and not having the required records at the required time can cause major problems in society. If an unauthorized person logs into the system as an administrator, they will have the authority to make required changes to the system or the data within the system to make criminals seem innocent and to make innocents look like criminals.

The proposed system from this research proposal is to implement a new method of authentication to enhance security. Since authentication systems run separately, this proposed system can be implemented on other applications to enhance their security. This proposed authentication system can be used on an industrial level and on an individual level for social media applications and other software that requires higher security to protect information stored within the systems. Existing higher authentication systems are costly and too complex to handle. With the proposed system for authentication, it will be easier to handle and will not cost compared to the existing systems.

2.2. Specific Objectives

To successfully implement a Multi-Factor Authentication (MFA) system for the Blockchain-Based Criminal Information Management System, there are some key areas that need to be looked into, and they would be;

- The first factor
- The second factor
- The third factor

2.2.1. The first factor

For every login scenario, the first factor will always be the entering of the username and the password [9]. All users who are using an account or would like to be using one in the near future are informed of using a strong password with letters (upper and lowercase), numbers, and special characters. Programmers have taken password security to a higher level, but still, individuals tend to use passwords that they can easily remember, and they keep on using the same password for several accounts so it would be easier for them to remember.

But the issue with the first factor is that once it is cracked, exploited, or guessed, there is nothing that the user can do to protect the data or information that were stored within that account. Hackers can use phishing methods and social engineering methods to trick the user into providing the required login credentials to a legitimate-looking site that is being controlled by the hacker. There is the oldest method of hacking a password, brute force attacks.

2.2.2. The second factor

While the first factor provided such weaknesses, developers and cybersecurity specialists improved the first factor by adding an extra layer of protection over that. The additionally added security layer or the second factor is normally a randomly generated number that is shared with the user’s mobile device to verify and confirm the login process.

But with SIM Swapping, cloning, and screen monitoring technology, the attacker can get the required details from the user even without the user knowing. The mentioned random generator number is a generator from some sort of server, and another way to receive these randomly generated numbers is from an application that is so-called an authentication app. These authentication apps and services that provide random codes could or would have vulnerabilities within the systems or the servers that the hackers could investigate and exploit. These kinds of vulnerabilities and threats make the second factor unsafe, and it brings some doubt to the users.

2.2.3. The third factor

With the second factor having security issues, cyber security specialists and developers investigated how to improve authentication to a much more secure way. As a solution developer and cyber security specialist came up with a unique feature for individuals that they can use as authentication. The inherent factor developers and security specialists improve security to a level that the user needs to provide their fingerprint, voice, face, or eye to access the required systems.

The ever-evolving technology brought Artificial Intelligence (AI) to a peak level; by providing pictures of a user, Artificial Intelligence (AI) can generate that user’s face in a real-looking way that would be difficult for anyone to identify. Artificial Intelligence (AI) has improved to the level that it can get audio recordings of any user and generate any word in the way the real user would speak. If properly performed, the user's fingerprint can be taken off from a glass that the user is holding onto or from your mobile screen. With these kinds of issues and technological improvements, having inherent factors to keep you safe from hackers would not be enough.

2.2.4. Proposed solution

The proposed solution is to develop a multi-factor authentication system with solutions to the existing factorial matters to heighten the security of the Blockchain-Based Criminal Information Management System. Since authentication systems are built separately, this system and the method of this system can be used for other applications to heighten their security and protect the users who are using those systems. Let’s look at how this proposed solution executes with each factor discussed in sections *2.2.1*, *2.2.2*, and *2.2.3*.

The first factor - most commonly, is the username and password for a website or a system. According to *BitWarden, Inc,* providing a password of 14 characters of random string values would be approved by the National Institute of Standards and Technology (NIST) [10]. Since 14 characters are long, most websites do not go for that number but rather use a number of 8 or 9 characters as the password. This proposed system will require passwords of 14 to 16 characters, with four character sets as follows;

- Numerical characters
- Lowercase characters
- Uppercase characters
- Special characters

This will increase the time a hacker would take to crack the password in brute focus attacks, figure 2.2.4. 1 will show this in a graphical method. But, even increasing the number of characters for the password would not be secure since hackers can be exposed and trick the user into providing them the password through phishing attacks and social engineering attacks. Those security issues take us to the second factor.

The second factor - when usernames and passwords started to get exploited, a new method was introduced. This method contained a 6-digit code that was sent to the user’s mobile or email to verify the authentication. But the limitation in that factor is that there are only 59,049 possibilities that a 6-digit code can generate. These 59,049 possibilities can be cracked with the proper computers with the required computational capabilities. There have been incidents where the authentication app itself had vulnerabilities, and the generated random code was exposed to hackers.

To increase security and to lower the possibility of being exploited, the proposed authentication system will move from the 6-digit code to a 6-character code. By shifting to a 6-character code, there will be 60,466,176 possibilities. This method would generate 1024 times more codes than the 6-digit code. With that, the time needed to exploit or crack such a passcode would take a significant amount of time, human resources, and computational power.

For example: if it took 10 seconds to generate all the 6-digit codes, it would take 10240 seconds (roughly 2 hours and 50 minutes) to generate all the 6-character codes.

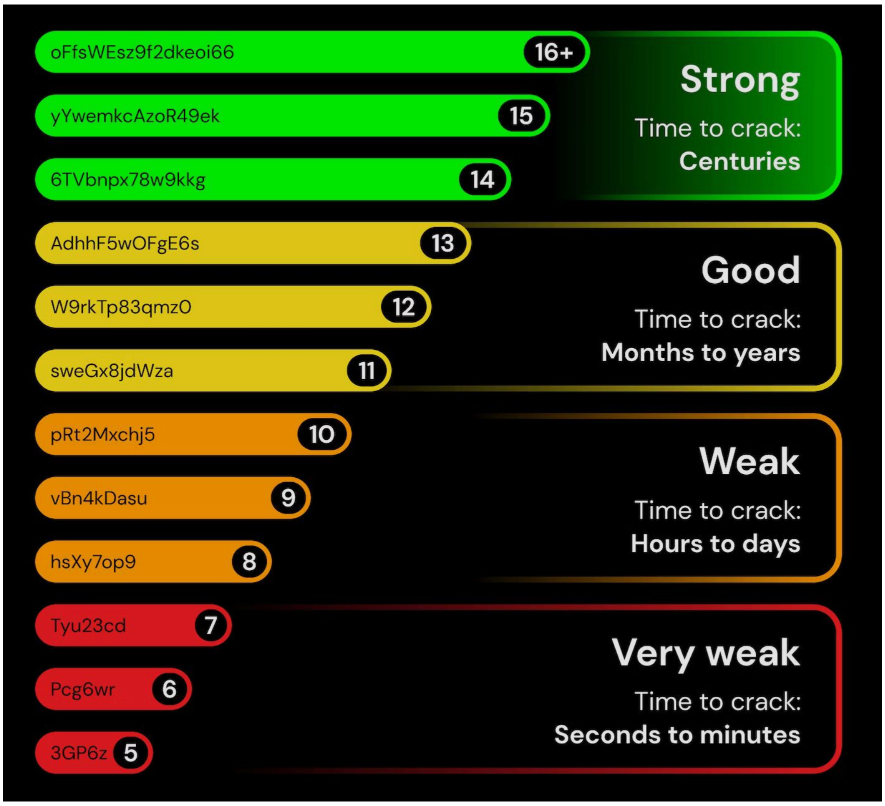

Figure 2.2.4. 1: Password strength according to the number of characters

Source: The Bitwarden Blog / How long should my password be? [11]

The third factor - if the third factor gets exploited, or the hacker obtained the 6-character code by an indirect method, such as SIM swapping, cloning, or simply exploiting a weak password you process on your email account, the third factor will provide the required next line of security. After the user has completed both the first and second factors, the user will be directed to complete the third factor, or in this project, that would be the last factor. We used the most common username and password on the first factor, and in the second factor, we executed the one-time password OTP code. The third factor will be using the Inherence factor with a simple extra layer of protection.

Facial recognition would be the inherent factor for the third factor that should be used in the authentication system. With proper training, artificial intelligence (AI) can be trained to identify faces that are animated using artificial intelligence, masks that are created to imitate a user, and the difference between those with the natural face. After verifying and moving forward with the facial recognition scan, the user will have to enter a certain pin code as the final step to reach the required system. This pin code that the user will have to enter will be unique to every user, and there will be a timer for this code to expire. After expiration, the system will generate another unique code for the users.

4. METHODOLOGY

Developing an Authentication System for any system requires a deep understanding of how the authentication system works and how the internal components and techniques work. The internet holds sufficient information about authentication and the algorithms that are used to develop them. Data and methods of performing the task and successfully getting results will be mainly gathered from the internet through Research papers and knowledge articles. When times that it looks like we are stuck and can not move forward, advice and guidance will be taken from the supervisors and seniors in the relevant fields. Additionally, technological advancement will be used to get ideas and guidelines.

The proposed system will have three factors with an additional security feature. The first factor is the standard username and password every application and system provides. The second factor is the improved OTP code that would provide 60,466,176 possibilities rather than the usual 59,049 possibilities. The third factor is the AI-powered facial recognition system to identify and verify the actual user.

If you look at each factor with more detail,

- When it comes to usernames and passwords, there are general policies that are globally recognized. So, when developing this factor, create policies and standards to ensure the strength of the password to be maximum. With these policies and standards, we can drive the users to create strong passwords with the requirements that are needed. Following are some policies and standards that can be implemented to stop users from creating weak passwords that are likely to be exploited [12].
    - Minimum and maximum length
    - Character restrictions
    - Frequency of password reuse
    - Disallowed user names or user IDs
    - Specify a minimum password age
- When it comes to the one-time password (OTP), the existing method of generating a random 6-digit code will be upgraded to generating a random

6-character code. This random 6-character code will be a combination of digits, uppercase letters, lowercase letters, and special characters. Table 4. 1 will provide the mentioned characteristics. By improving the code to such length, we will be increasing the time for a hacker to exploit the code via brute focus attack 1024 times harder. Since the code would be random, the only other way the hacker or an attacker can get the code is through the user; this could be done through phishing, social engineering, SIM swapping, and cloning methods.

Digits	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Uppercase Letters	A, B, C, D, E, F, G, H, I, … R, S, T, U, N, M, X, Z, Y
Lowercase Letters	a, b, c, d, e, f, g, h, i, … r, s, t, u, n, m, x, z, y
Special Characters	!, @, #, $, %, ^, &,*, (,), -, _, =, +, <, >, /, ?, \, |, [,], {, }

Table 4. 1: 6-Character Code Characteristics

- When it comes to facial recognition, it will be an AI-powered scanner to identify the real user from hackers or attackers who are pretending to be the user with masks, pictures, and other AI-powered facial tools. This factor will stop any attacker or hacker that could bypass or exploit the first and second factors. The required data for the AI-powered scan will be collected over the internet, and some data that could be used to train the AI tool will be collected from the project group, family, and friends. When the facial scan has been passed, the user will enter the final security feature, which would be to enter a unique code that is generated from the system that only the user would know.

Successfully completing all the authentication steps would grant the user access to the blockchain-based criminal information management system. For this project, we have gone the extra mile for the authentication security since the authentication part can be used separately on any other system or software where authentication is required.

4.1. Authentication System Overview

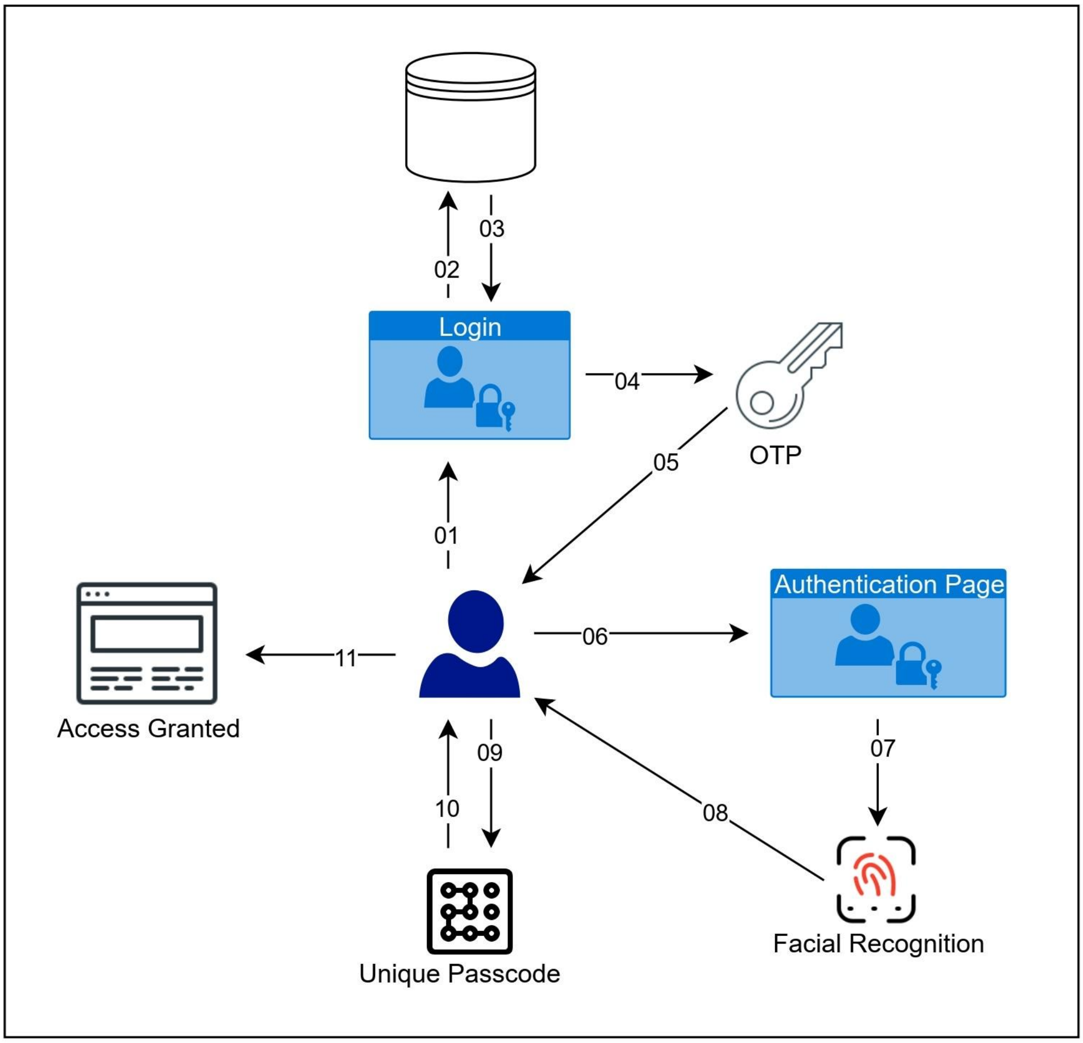

Figure 4.1. 1: Authentication System Overview

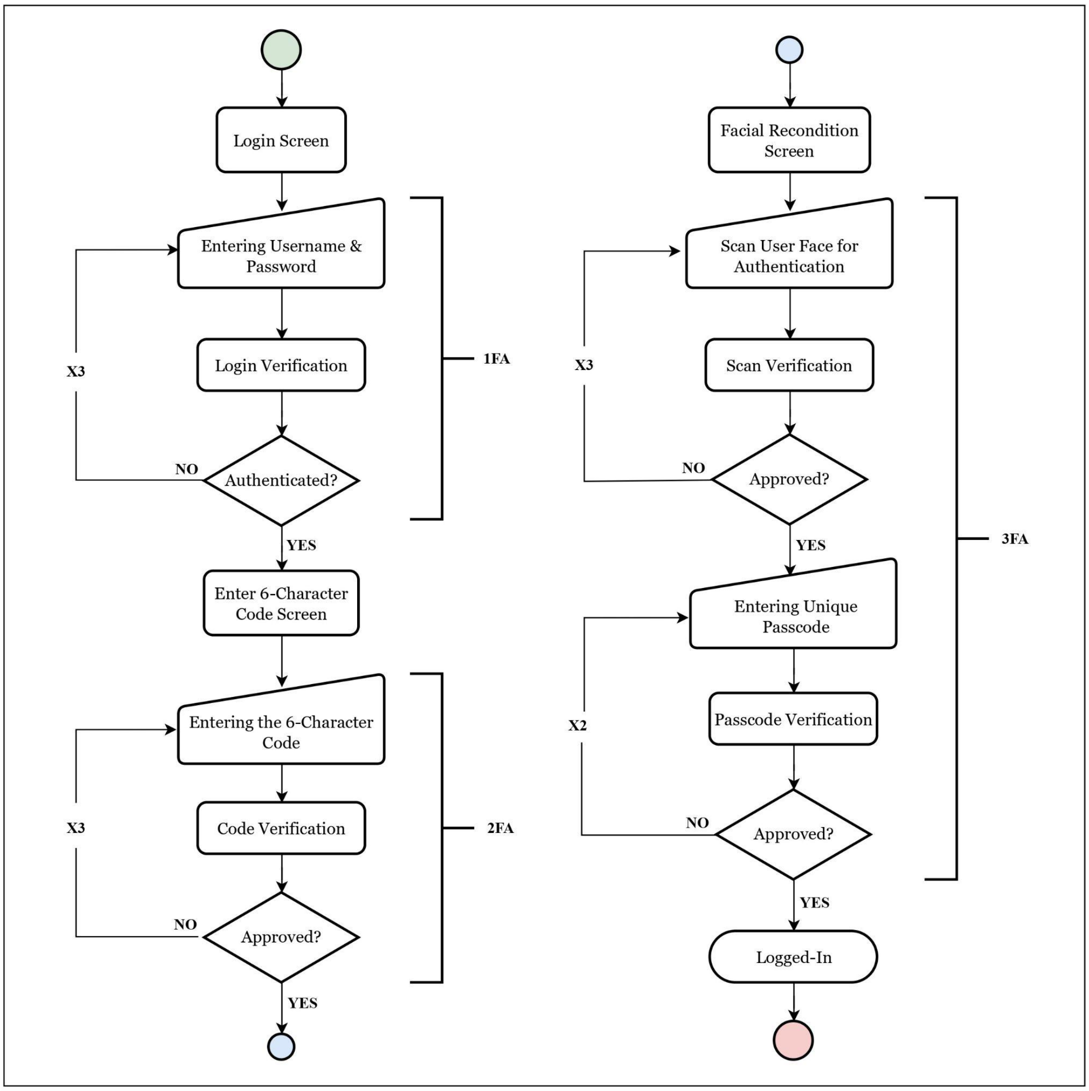

Figure 4.1. 2: Authentication System Overview - Flow Chart

4.2. Proposed Technologies

Following technologies will be proposed to develop the solution, but with the implementation, their proposed technologies might defer.

- HTML
- JS
- CSS
- Python
- OpenCV
- HMAC Algorithm
- Encryption
- Decryption

Table 4.2. 1 will display the proposed reasons for using the mentioned technologies to develop the authentication system for the blockchain-based criminal information management system.

Technology	**Reason**
HTML	To describe the structure of the web pages.
JS	To create dynamic and interactive web content like applications and browsers.
CSS	To describe the presentation of Web pages, including colors, layout, and fonts.
Python	Will be used as the main programming language.
OpenCV	To provide a common infrastructure for computer vision applications and to accelerate the use of machine perception in commercial products [13].
HMAC Algorithm	To achieve authentication and verify that data is correct and authentic with shared secrets [14].
Encryption	To protect the confidentiality of digital data stored on computer systems or transmitted over the internet or any other computer network.
Decryption	To convert the encrypted data into its original form.

Table 4.2. 1: Proposed technologies and reasons to use them

4.3. System Development Process

The Agile software development methodology will be utilized for the proposed solution's development. The ability to adapt and respond to change is referred to as agile software development. Figure 4.3. 1, will provide an explanation of the development process.

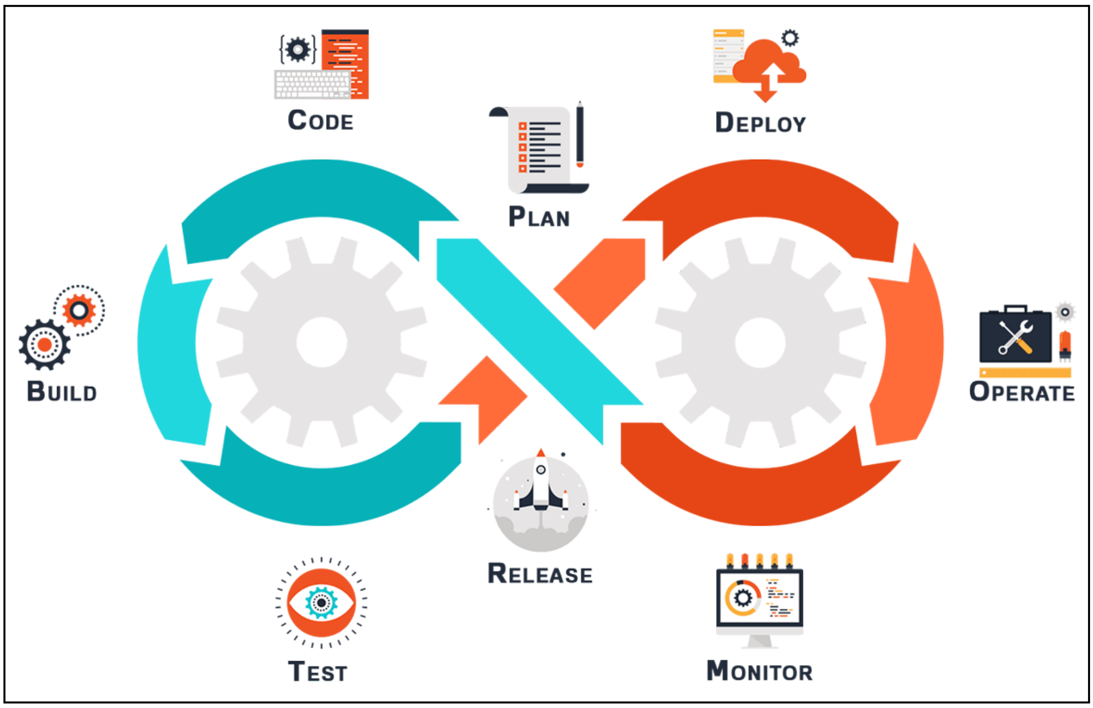

Figure 4.3. 1: Agile Software Development Methodology

Downloaded from PNGEGG [15]

Embracing change while providing usable software to the stakeholders is the ultimate aim of the Agile process. The Scrum technique will thus be used instead of the other agile approaches that are available.

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 [16].

4.4. Gantt Chart

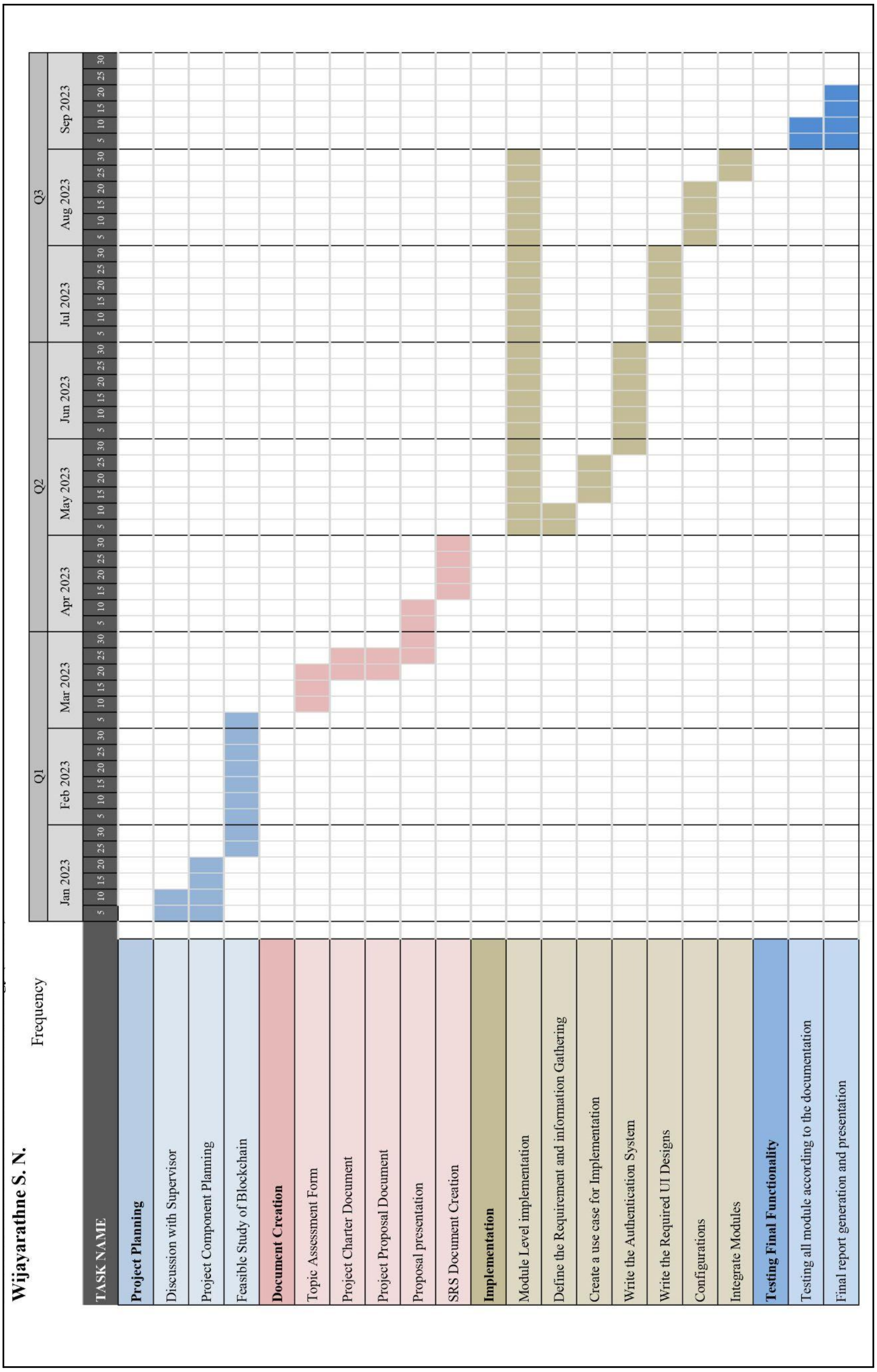

Figure 4.4. 1: Gantt Chart

5. PROJECT REQUIREMENTS

5.1 Functional Requirements

- This proposed authentication system needs to follow password standards and policies.
- This proposed system needs to provide user limitations for the number of attempts they can enter the password and username incorrectly.
- This proposed system needs to provide user limitations for the number of attempts they can enter the 6-character code incorrectly.
- This proposed system needs to provide user limitations for the number of attempts they can fail in the facial detection authentication segment and the number of how many times they can enter their unique code incorrectly.
- This system should be able to access the camera of a laptop or an external web camera of a monitor for the facial detection authentication segment.
- This system should have a secure and complex algorithm to generate the required 6-character codes in randomized order.
- This system should provide a tier for the 6-character codes authentication segment for the user to enter the code within the timer, or the code would be useless.

5.2 Non-Functional Requirements

- This system is to be expected to executive flawlessly by performing well.
- Since the internal system, namely the blockchain-based criminal information management system, contains confidential details and information, there will be a timely restriction activated.
    - For example, the users, namely the citizens, will have 24x7 access to report anything suspicious or to report crimes. But, admin-level users will have their accounts activated during working hours to limit their functionalities within the system after the working duration. If needed, access needs to be 'VIEW ONLY' after working hours.
- This authentication system needs to be user-friendly for any citizen with even no prior knowledge regarding computers to easily understand.

6. COMMERCIALIZATION PLAN

6.1 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
    - Civilience
    - Victims
    - Law Enforcement
    - Police Officers
- Social Media Applications
- Hospitals
- Police Departments
- Vulnerability Scanning Tools
    - Example: Acunetix
- Cyber Security Monitoring Tools
    - Example: CrowdStrike

6.2 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.