BLOCKCHAIN-BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA: AUTHENTICATION SYSTEM

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

September 2023

BLOCKCHAIN-BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA: AUTHENTICATION SYSTEM

Wijayarathne S. N

(IT20171438)

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

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

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. I would like to express our sincere gratitude to everyone who contributed to this study. I 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.

Finally, I 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

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,

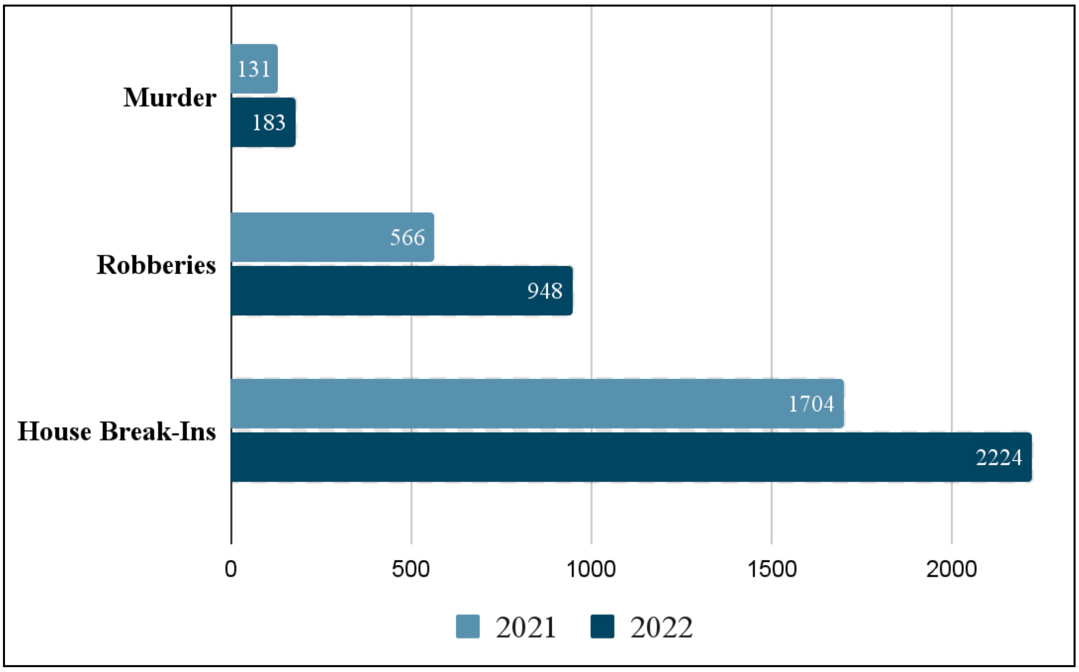


Figure 1.1. 1: Reported crimes in the first four months of 2021 and 2022

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.

1.3. 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];

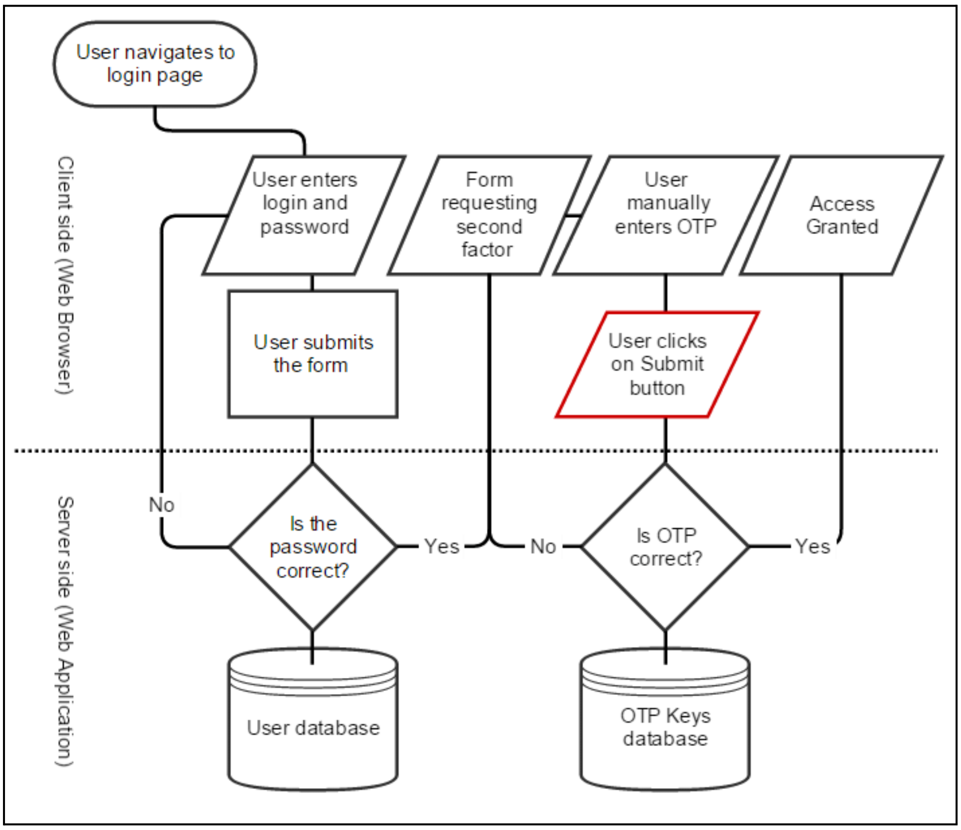

User navigates to login page
Client side (Web Browser)
User enters login and password
Form requesting second factor
User manually enters OTP
Access Granted
User submits the form
User clicks on Submit button
Server side (Web Application)
No
Is the password correct?
Yes
No
Is OTP correct?
Yes
User database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

1.4. Research Objectives

1.4.1. 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.

1.4.2. 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

1.4.2.1. 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.

1.4.2.2. 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.

1.4.2.3. 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.

1.4.2.4. 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.

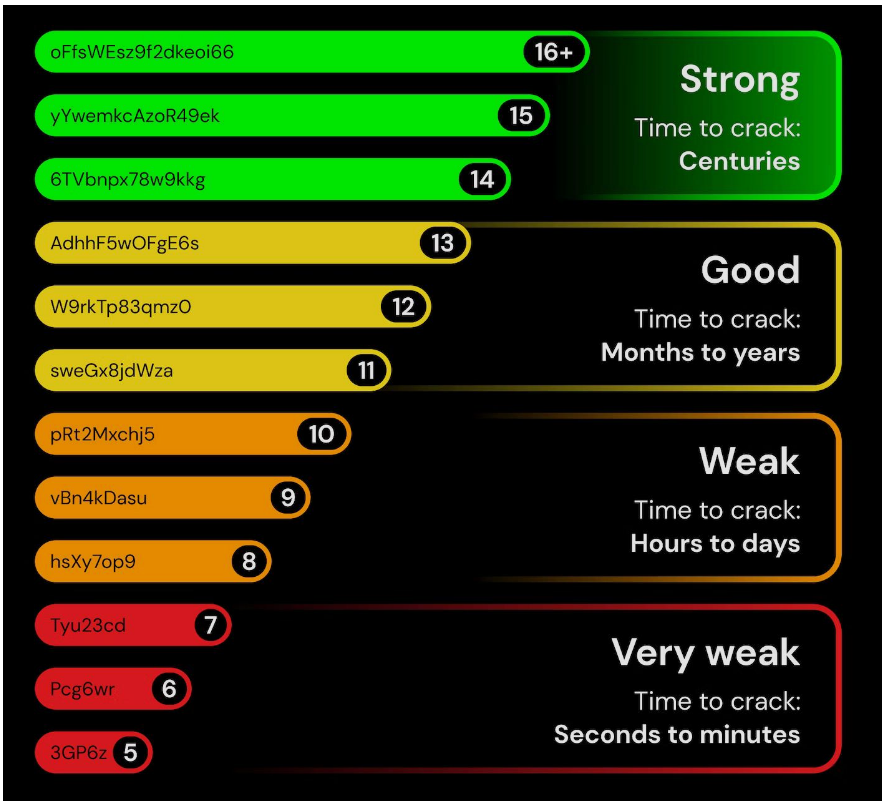


Figure 1.4.2. 1: Password strength according to the number of characters

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.

2. 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 2. 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.

2.1. Authentication System Overview

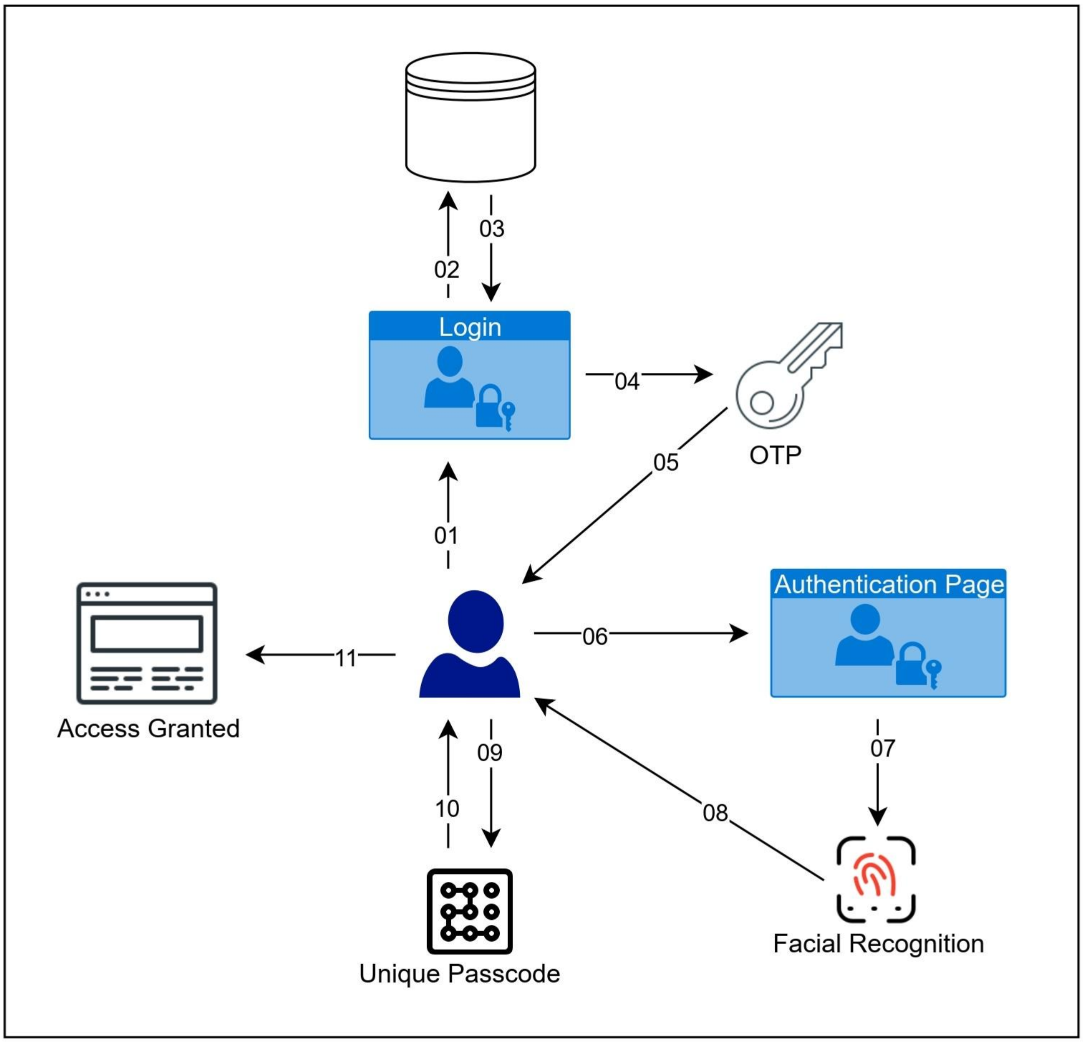


Figure 2.1. 1: Authentication System Overview

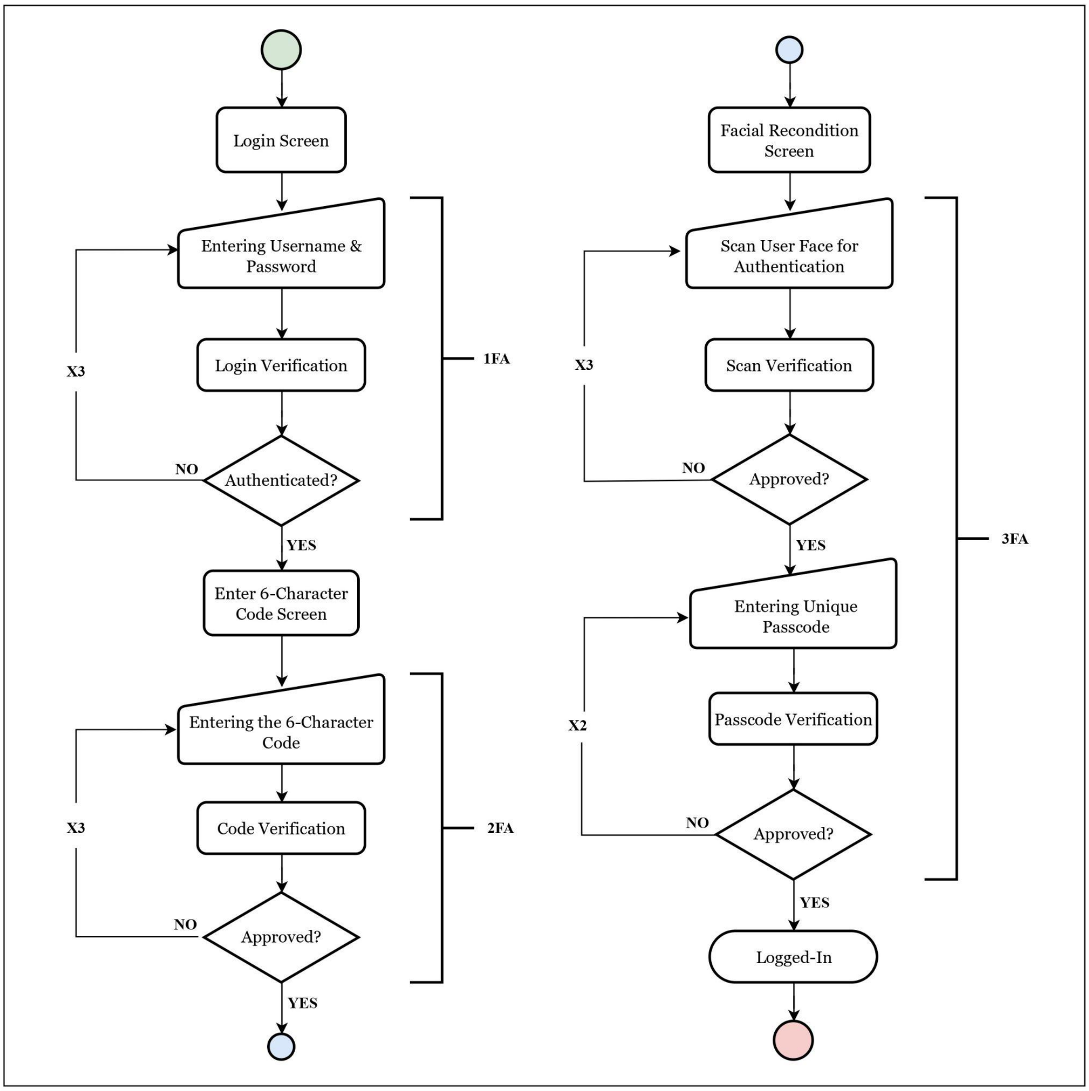


Figure 2.1. 2: Authentication System Overview - Flow Chart

2.2. Research: Implementation of an Authentication System

With the idea of introducing a new mechanism for an Authentication system, there came the need to research whether this change would be sufficient for the citizens of Sri Lanka after being used to the existing method. So, with the required requirements, a research was conducted to determine the basic technological advancement.

With the introduction of this new authentication system, there would be some technological requirements that need to be fulfilled to comprehensive this system. The technological requirements are as following;

- Should be compatible with the world wide web and internet connections.
- Should have an active internet connection.
- Device compatible with facial recognition functionalities;
    - Mobile: mobile camera
    - Laptop: laptop camera or an external camera
    - Desktop: external camera

A collaborative research was done along with 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] during the following time duration to collect required details from the citizens of Sri Lanka regarding the proposed Authentication System, with the needful functionalities.

- Start date to collect data: 25th of May, 2023
- End date of data collection: 30th of June, 2023

Since any authentication system is being used by all age groups, this research was conducted to gather details from a vast variety of different age groups of citizens in Sri Lanka, and the following are the age groups that was considered for this additional research;

- Age below 16 years
- Age between 16 to 25 years
- Age between 26 to 35 years
- Age between 36 to 45 years
- Age between 46 to 55 years
- Age above 55 years

With the selected age ranges, this research survey was able to collect numerous data that was taken into consideration while moving forward with this research.

Based on the responses that were received by the end date of the ‘Implementation of an Authentication System’ research, this survey has reached a total number of 102 individuals and those 102 individuals have been spread upon all the age ranges by making this research survey a success.

If we look into the data that was received, we can see this survey has been conducted by the number of following individuals;

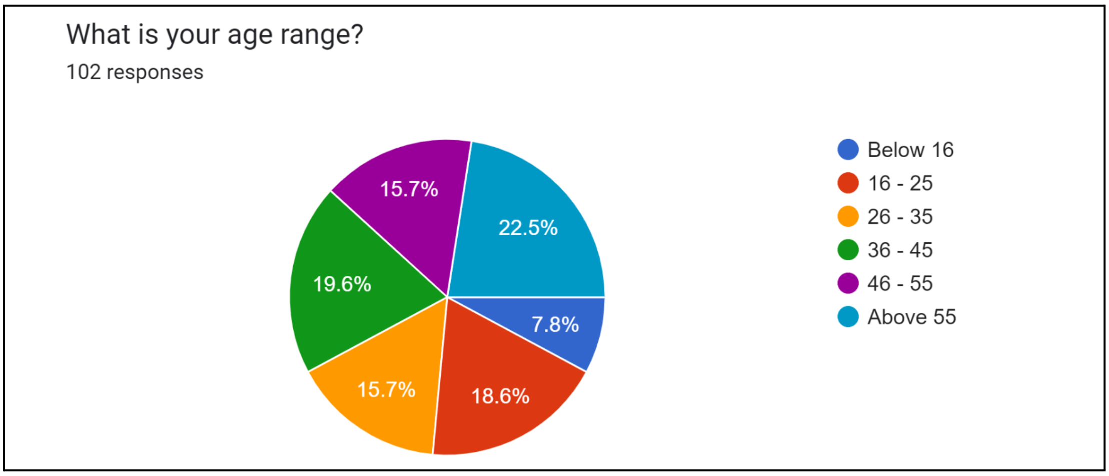


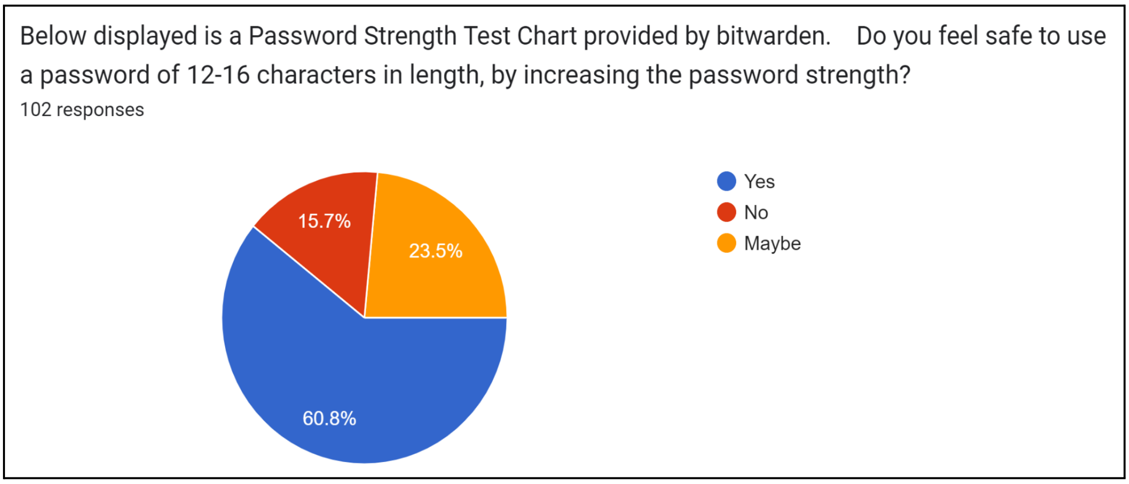
Figure 2.2. 1: What is your age range? [From the survey]

Age range	Percentage	Actual number
Below 16 years	7.8%	08

Between 16 to 25 years	18.6%	19
Between 26 to 35 years	15.7%	16
Between 36 to 45 years	19.6%	20
Between 46 to 55 years	15.7%	16
Above 55 years	22.5%	23

Table 2.2. 1: What is your age range? [From the survey]

With the vast very of ages have completed the survey, they were asked about their thoughts of increasing the password character length, so the password should be in between 12-16 characters, the following was the responses that were received;



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?

102 responses

Figure 2.2. 2: Question about the password of 12-16 characters [From the survey]

During the same research, questions was asked to identify the following key aspects that any user should have to properly use the proposed authentication system;

- How familiar are you with facial recognition systems?
- Are you comfortable with using a system that has a Facial Recognition System implemented?
- Are you comfortable with using a system that has a Facial Recognition System implemented?
- Provide a reason why you believe that Facial Recognition Systems should have been implemented on the above mentioned time?

Based on the answers that were provided for these survey questions, the research that was conducted had to be questioned, and had to be changed to fulfill the needs and the technical background of the citizens of Sri Lanka. The answers for the above-mentioned questions are as follows;

Question: How familiar are you with facial recognition systems?

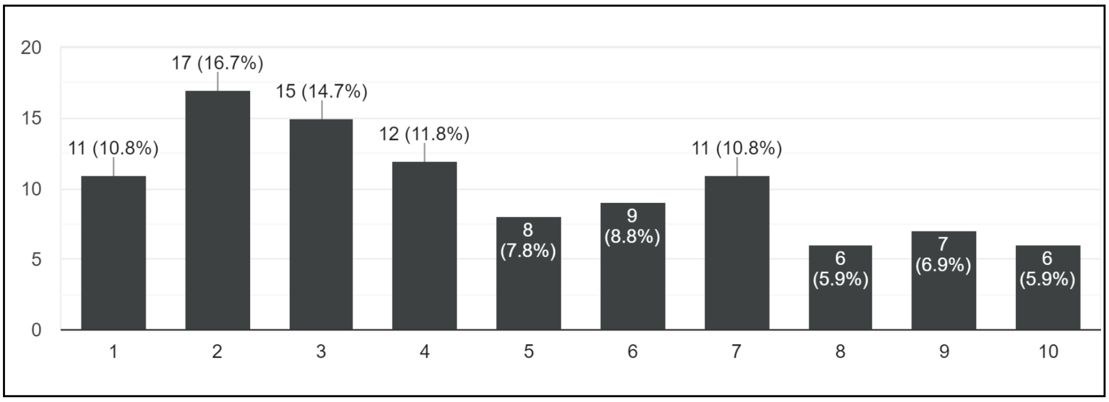


Figure 2.2. 3: How familiar are you with facial recognition systems? [From the survey] [1:Rookie, 10:Expert]

With over 60% of the individuals providing a rank less than 5 out of a ranking of 10, the implementation of the facial recognition system was in question. Since this system is developed for the citizens of Sri Lanka, this was a major bottleneck when it comes to the implementation of the 3rd factor of the authentication system.

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

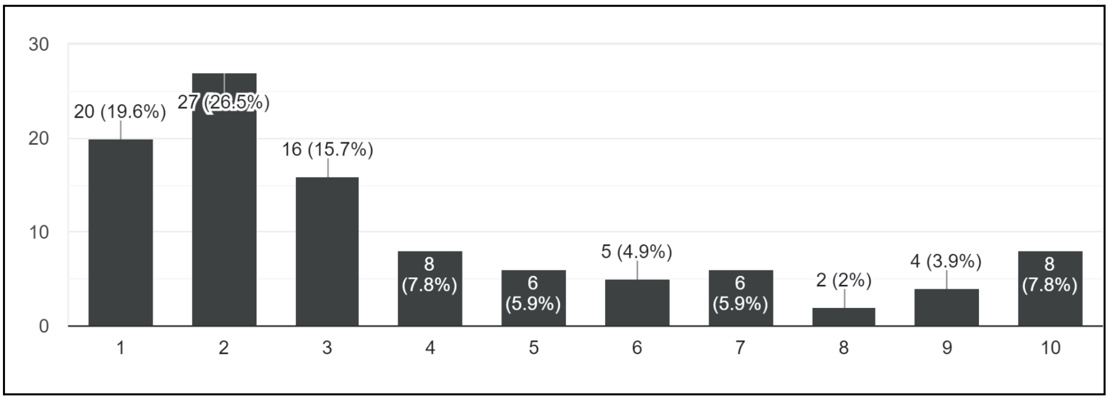
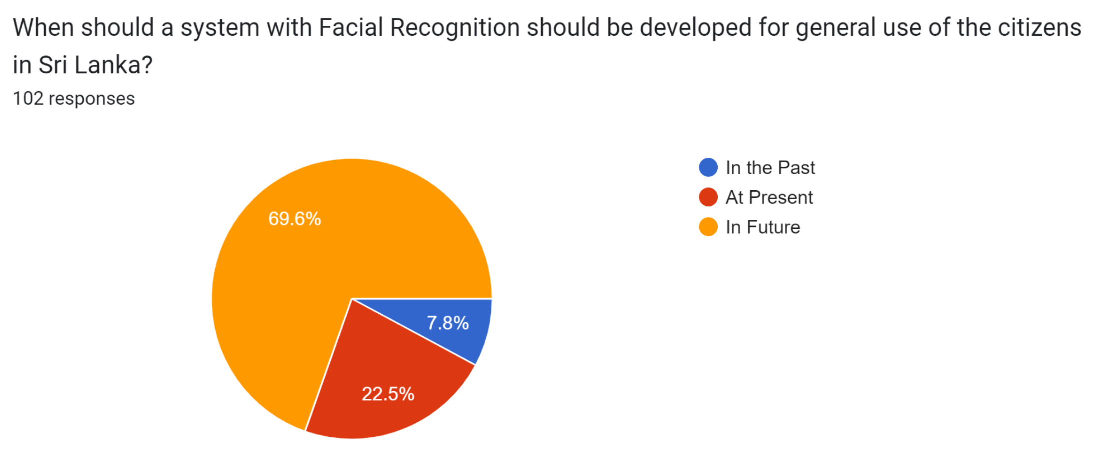


Figure 2.2. 4: Comfortability of using facial recognition systems? [From the survey] [1: Not Comfortable, 10: Highly Comfortable]

With more than 75% of the individuals providing a rank less than 5 out of a ranking of 10, it was identified that the citizens of Sri Lanka are not comfortable with using a system with facial recognition. Since this authentication system is provided on a blockchain-based criminal information management system, without the individuals not being comfortable, the system might not be used and the purpose of the entire system would be at jeopardy.

With this, a hard decision had to be made regarding the authentication system, and that was to move forward without the facial recognition system. With more than 60% of the individuals not being familiar with facial recognition systems and more than 75% of individuals not comfortable with the use of a facial recognition system, this proposed method had to be changed to match the needs and requirements of the citizens of Sri Lanka.

During this research survey, another question was asked based on when should a system with facial recognition should be developed and implemented for the general use of; and the following are the answers that was received;



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

102 responses

Figure 2.2. 5: Time period to develop Facial Recognition [From the survey]

- As ‘In the past’ the requirement was to see whether the respondents would suggest that these systems should already be implemented and should be in use.
- As ‘At Present’ the requirement was to see whether the respondents would

suggest that these systems should now be implemented and should be started to be used.

- As ‘In Future’ the requirement was to see whether the respondents would suggest that these systems should not be implemented now and should be kept for the future generations.

At the latter part of the survey, a combined question was raised linking with the above question, asking the respondents to provide the reason why they believe that the facial recognition system should be implemented in their mentioned time period. Following are some of the responses that was provided by the individuals;

Age Range	**Time Period**	**Provided Reason**
46 - 55	In Future	I think we should wait for the technology to become simpler. Right now, it feels too complex for folks like me in their 40s. By the time it's easy to use, we'll be more comfortable with it
Above 55	In Future	I've seen my kids use all these gadgets effortlessly, but it's overwhelming for me. Let them fine-tune it for our generation in the future.
16 - 25	At Present	As the crime rate is increasing in these times, it is beneficial for any shop/organization/entity to adopt a facial recognition system to strengthen the security in the said entity
36 - 45	In Future	I think it's important for the technology to be foolproof before we adopt it. We should wait until it's more reliable.
Above 55	In Future	I remember when phones were just for calling. Let the new generation handle the latest tech while I enjoy my trusted methods

26 - 35	In Future	I'm not sure I'd feel comfortable having my face scanned everywhere.

Table 2.2. 2: Reasons for the provided time period? [From the survey]

[Please refer to ‘Appendices A: Implementation of an Authentication System’ for further details about the above-mentioned research.]

2.3. System Changes based on the Research

With the mentioned research on the above section, the based research had to be shifted to meet the requirements of the citizens of Sri Lanka and their technical backgrounds, so the system could be used by any individual without any difficulties.

The base requirement was to create an Authentication System with three layers,

- With the 1st layer being the general username and password, advanced with restrictions and functionalities.
- The 2nd layer being the OTP code, improved with new functionalities to generate 1024 times more codes.
- And lastly the facial recognition system, with an AI trained module to increase the security of the authentication mechanism.

After analyzing the results that were received from the conducted online survey; It is clear to say the implementation of the facial recognition system would not be beneficial for the citizens of Sri Lanka and it would be an implementation that would restrict the individuals from using the main system itself.

Update or else the change requirement would be as following;

- With the 1st layer being the general username and password, advanced with restrictions and functionalities
- The 2nd layer being the OTP code, improved with new functionalities to generate 1024 times more codes.

Considering this changed requirement and the existing solutions, we can surely say that this proposed system will have a higher level of security than the existing methods.

2.4. 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.

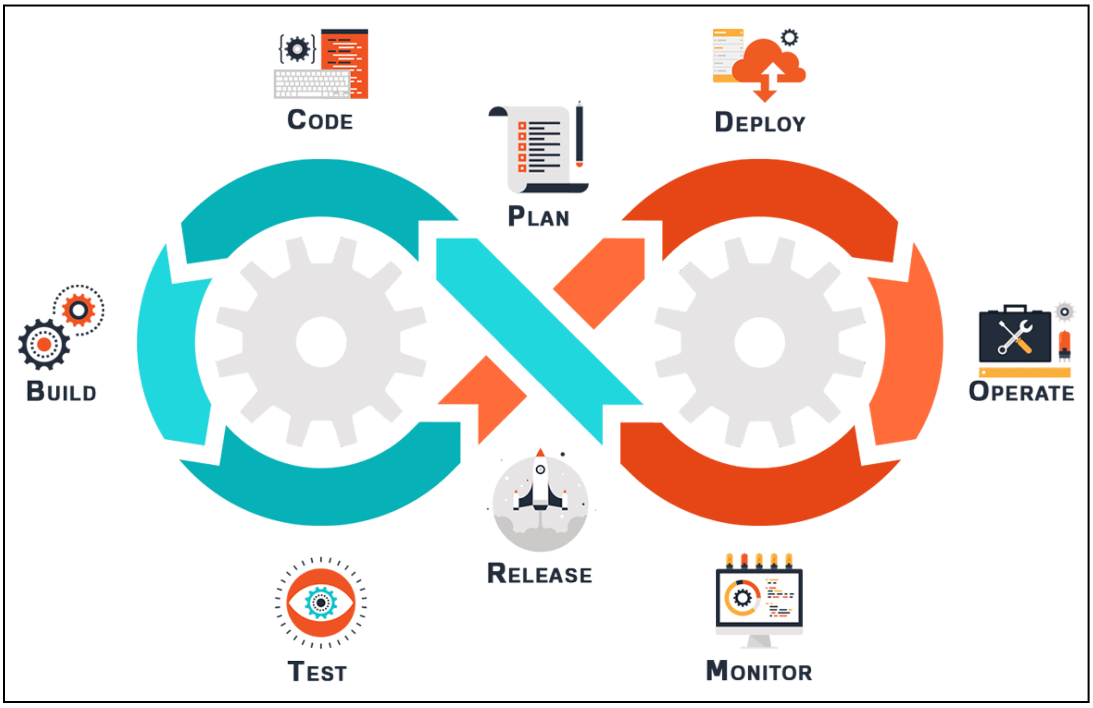


Figure 2.4. 1: Agile Software Development Methodology

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].

2.5. Commercialization Plan

2.5.1. 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
    - Law Enforcement
    - Police Officers
- Social Media Applications
- Hospitals
- Police Departments
- Vulnerability Scanning Tools
    - Example: Acunetix
- Cyber Security Monitoring Tools
    - Example: CrowdStrike

2.5.2. 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.

My part in this enormous arrangement is tied in with ensuring the ideal individuals gain admittance - that is where the Confirmation Framework comes in. Consider it a better approach to control who can enter. It resembles tracking down the ideal harmony between keeping things safe and making them simple to utilize. My center was clear: I needed to plan a way for individuals to confirm their personality that feels truly smooth. The outcome? A framework that goes past the typical techniques, giving us heaps of new choices while keeping everything very protected.

In the pages that follow, the excursion through the plan, improvement, and arrangement of this Validation Framework unfurls. An excursion that enlightens the specialized ability saddled as well as the comprehension of a more extensive mission - to protect data and induce trust. As the digits of code united with the desire for a more secure tomorrow, 1024 extra OTP codes arose, a demonstration of the devotion to outperform impediments.

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. As we dive into the core of this execution, let us uncover how this computerized key opens entryways to information as well as to the commitment of a safer society.

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;

- HTML
- CSS
- Java Script
- Python
- HMAC Algorithm
- Encryption
- Decryption

With the bottlenecks that I had to face during the implementation and the documentations, and the system changes that were later done according to the collaborative research that was conducted along with 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], the initial gantt charts had to be changed and improved. Following are two gantt charts that are included with the following details mentioned;

- Figure 3.1. 1: Gantt Chart I (Initial gantt chart that was created during the start of the project)
- Figure 3.1. 2: Gantt Chart II (Updated gantt chart based on the collaborative research that was conducted)

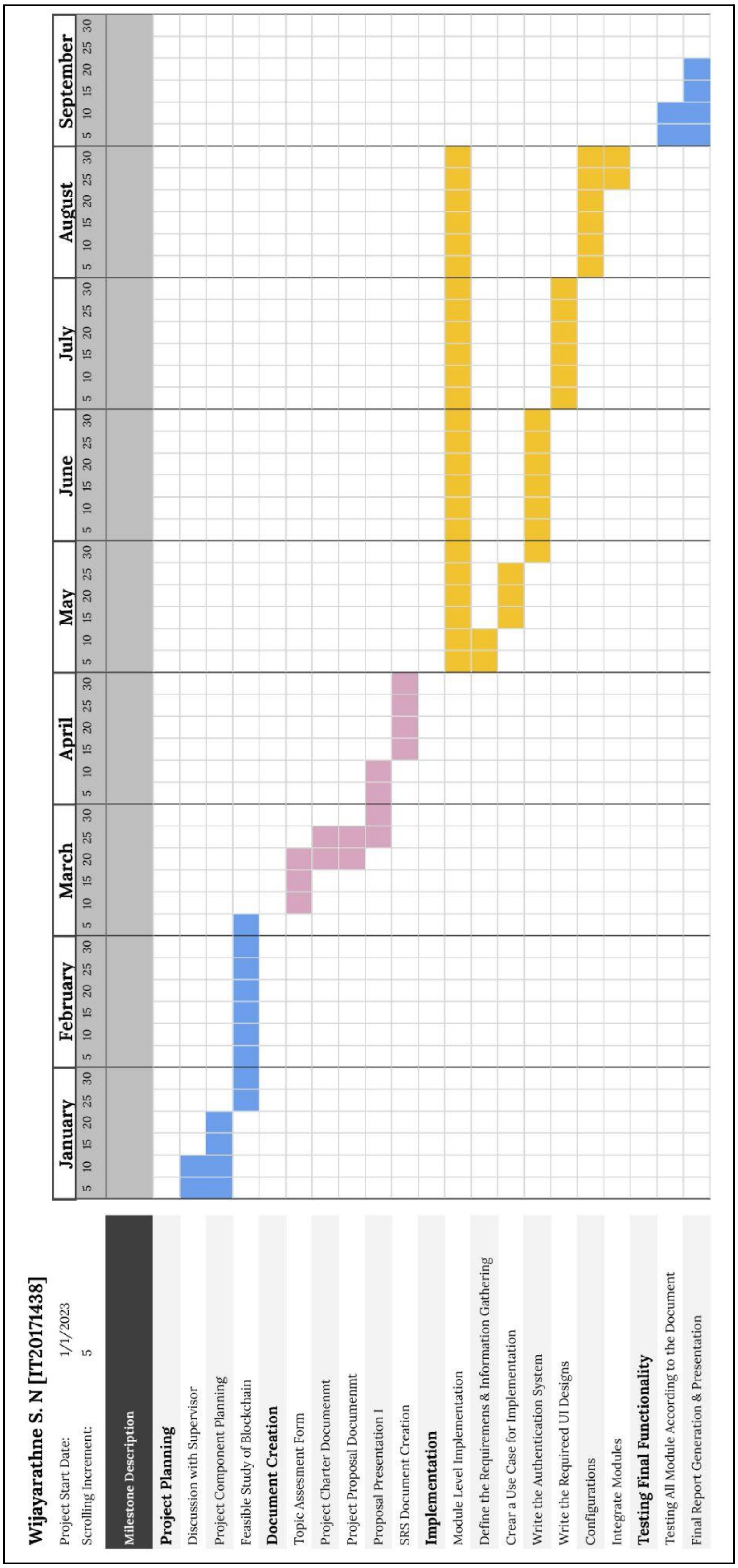
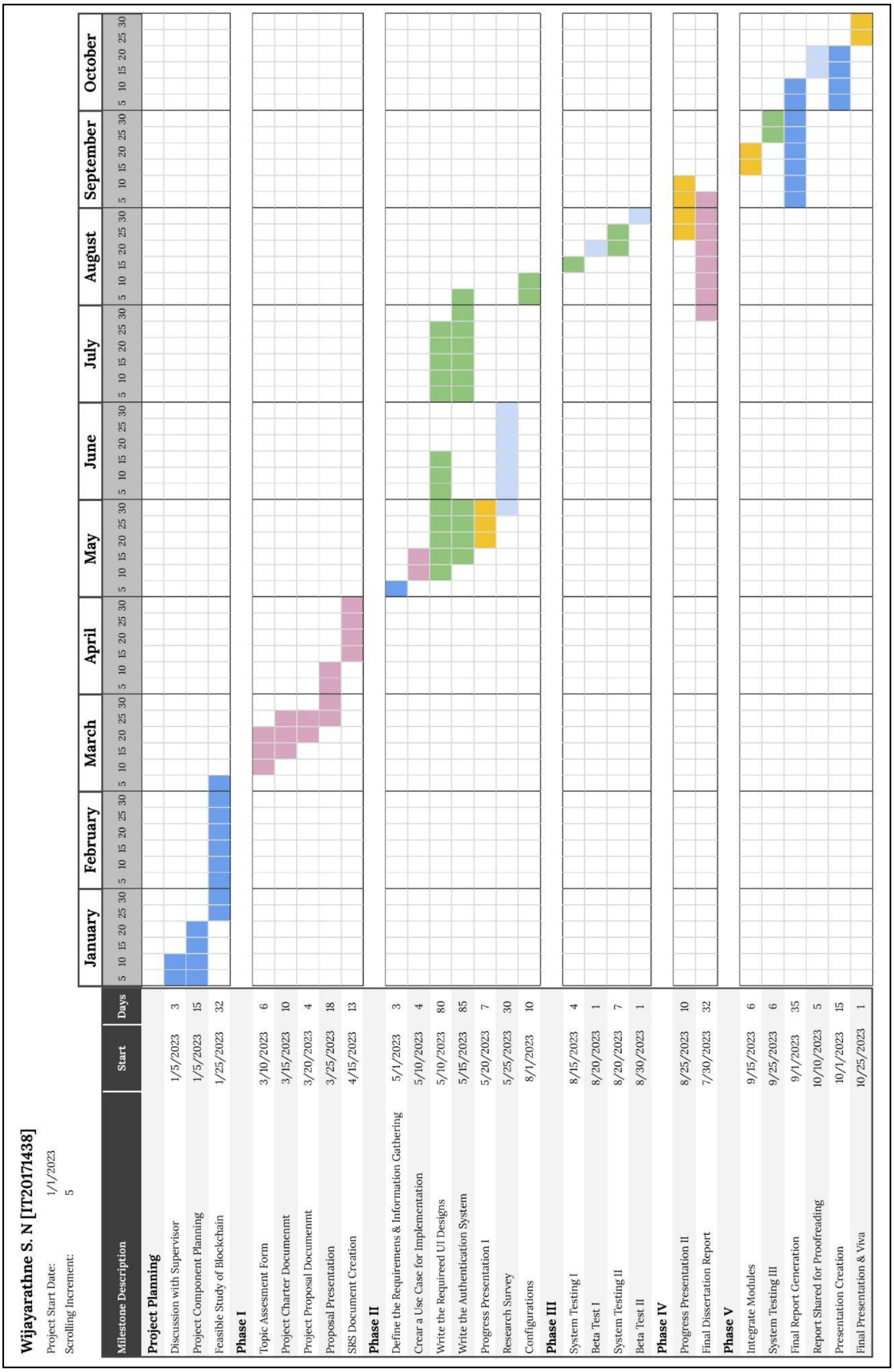


Figure 3.1. 1: Gantt Chart I



Wijayarathne S. N [IT20171438]

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 Documennt	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
Write the Authentication System	5/15/2023	85
Progress Presentation I	5/20/2023	7
Research Survey	5/25/2023	30
Configurations	8/1/2023	10
Phase III		
System Testing I	8/15/2023	4
Beta Test I	8/20/2023	1
System Testing II	8/20/2023	7
Beta Test II	8/30/2023	1
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. 2: Gantt Chart II

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.		

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.		
	08/15/2023	Username/Password Authentication	Successful
	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.		
	08/16/2023	OTP Code Rules & Functionalities	Successful
	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.		
	08/16/2023	OTP Code Authentication	Successful
	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.		
	08/16/2023	Email Verification	Successful
	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 addresses.		

Table 3.2. 2: Security Related Testing

4. RESULTS & DISCUSSION

These following sections hold the comprehensive outcomes of the implemented authentication system with extended security. The base to collect these results was successful implementation of the authentication system that was done through hard work, sleepless nights, prior research papers, and a determination to not give up.

These findings, obtained through rigorous testing and analysis, shed light on the effectiveness of the system in enhancing security while ensuring user convenience. Since this is a system developed for the everyday use for the citizens of Sri Lanka, this system had to be developed so everyone could use this without trouble.

Even with the collaborative research done with 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] about the Implementation of the Authentication System, several other 'Beta Tests' had to be done to see the practical implementation of the system and see how the citizens of Sri Lanka would react to the new Authentication System.

These following sections contain the details and data that was gathered from the 'Beta Test', followed by a thorough discussion of the status of the research (successful or unsuccessful) and the potential avenues for future advancements and developments.

Additionally, I would like to show my gratitude to Ms. M. W. N. L. De Silva who supported me with the conducted collaborative research, as well as providing me a helping hand during the conducted 'Beta Test'.

4.1. Results from the 'Beta Test'

A Beta Test is a period of testing that a product or item goes through before its true delivery to the general population. During a beta test, a predetermined number of clients, frequently alluded to as beta analyzers, are welcome to utilize the product or item under certifiable circumstances. The essential objective of a beta test is to distinguish and redress any leftover bugs, errors, or ease of use that could have been neglected during before testing stages.

Beta testing gives important criticism from clients who associate with the product in different ways. This assists engineers with refining the item, upgrading its usefulness, and guaranteeing that it addresses the issues and assumptions for its target group. Beta tests can likewise assist with revealing potential security weaknesses and assemble bits of knowledge into client experience, prompting upgrades and improvements.

For this conducted Beta Test, a selected number of individuals (30 individuals) were selected from the following age groups; the total number was created by having 5 individuals from the same age group;

Age Group (Years)	**# of Individuals**
Below 16	5
Between 16 to 25	5
Between 26 to 35	5
Between 36 to 45	5
Between 46 to 55	5
Above 55	5
Total Number	**30**

Table 4.1. 1: Individuals based on age groups

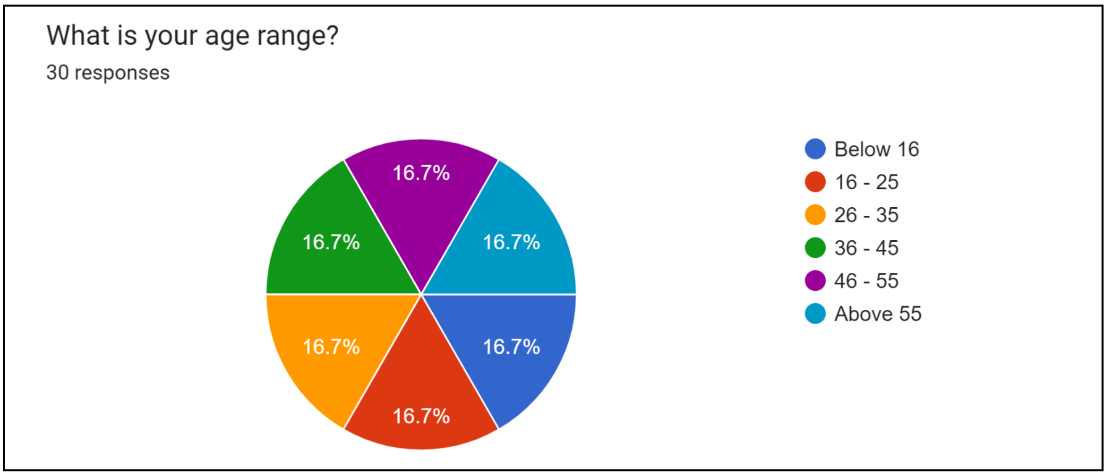


Figure 4.1. 1: Individuals based on age groups

The above-mentioned age groups were selected based on the previous collaborative research conducted by myself and Ms. M. W. N. L. De Silva, the exact age groups were used to get more efficient details and data.

During the Beta Test, five simple questions were asked after letting the 30 individuals finish the test. Following are the five ur simple questions were asked and recorded;

- How complex was this Authentication System to use?
- How satisfied were you with this Authentication System?
- Do you believe that this Authentication System will be more secure than the existing methods?
- How comfortable are you to recommend this authentication system to others?
- Would you like to provide any additional feedback/comments that can be used for further improvements of this system?

Following are the responses that were received from the Beta Testers for each question mentioned above;

Question: How complex was this Authentication System to use?

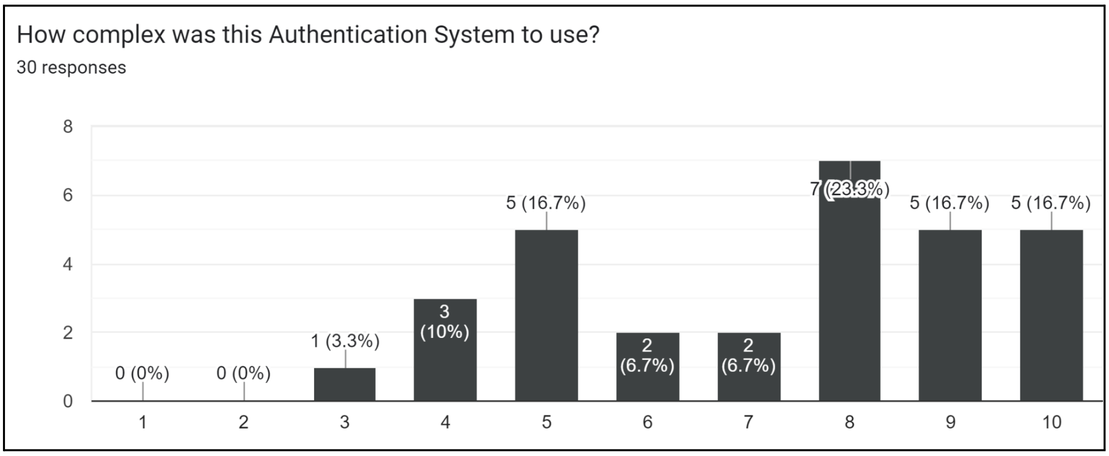


Figure 4.1. 2: Complexity of the Authentication System
[1: Complicated, 10: Straightforward]

With more than 70% (21 individuals) of the individuals rating the above the rating above 5; it can be said that the implemented Authentication System is Straightforward and simple to use.

Question: How satisfied were you with this Authentication System?

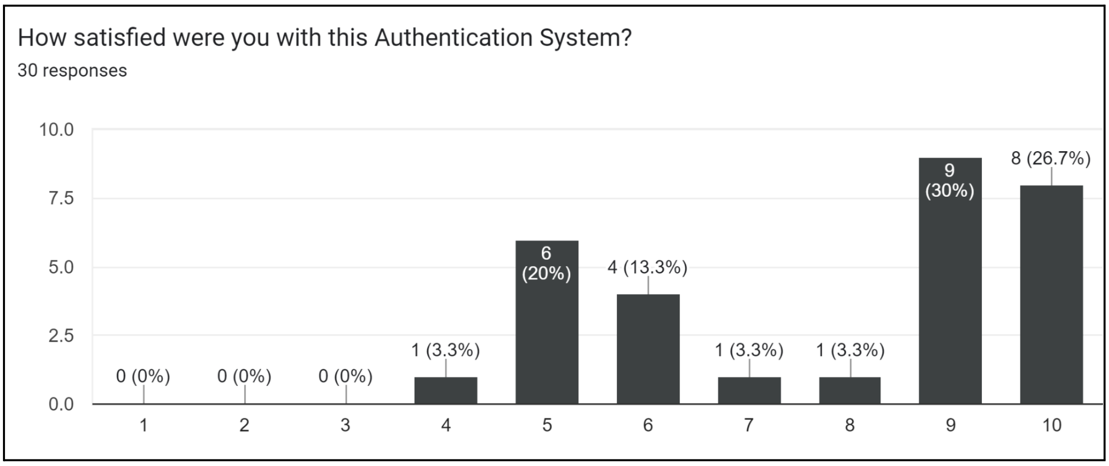


Figure 4.1. 3: Satisfaction for the Authentication System
[1:Unsatisfied, 10:Highly Satisfied]

With almost 100% of the individuals providing a rating above 5; it is clear that the Beta Testers were highly satisfied about the Authentication System and of its functionalities.

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

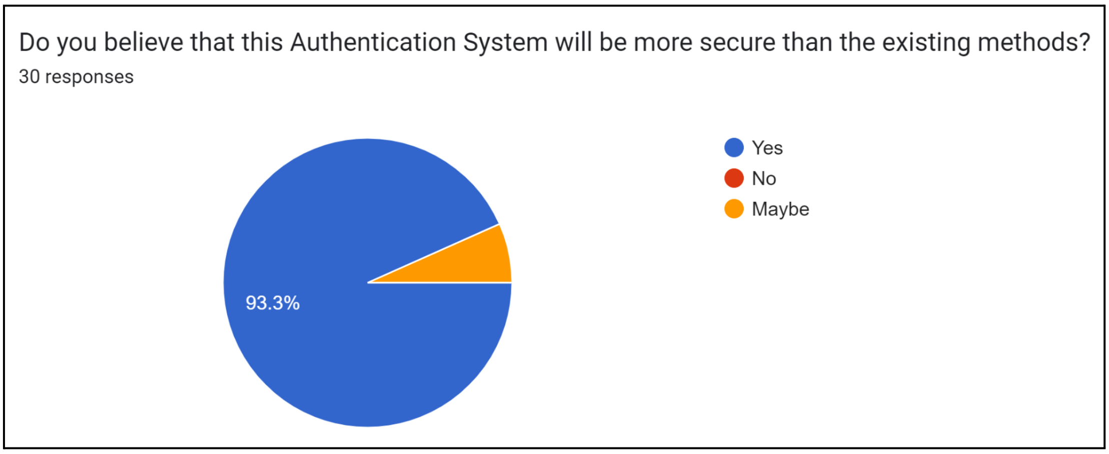


Figure 4.1. 4: Security of the Authentication System

With 0% negative responses, all the responders have agreed that this Authentication System would increase the level of security more than the existing methods, and would bring them to a state of having better online security. During the phase where I explained about the system, the individuals had some questions and doubts, but when shown facts, they understood that this system can reach new heights and provide better security for their personal lifes.

Question: How comfortable are you to recommend this authentication system to others?

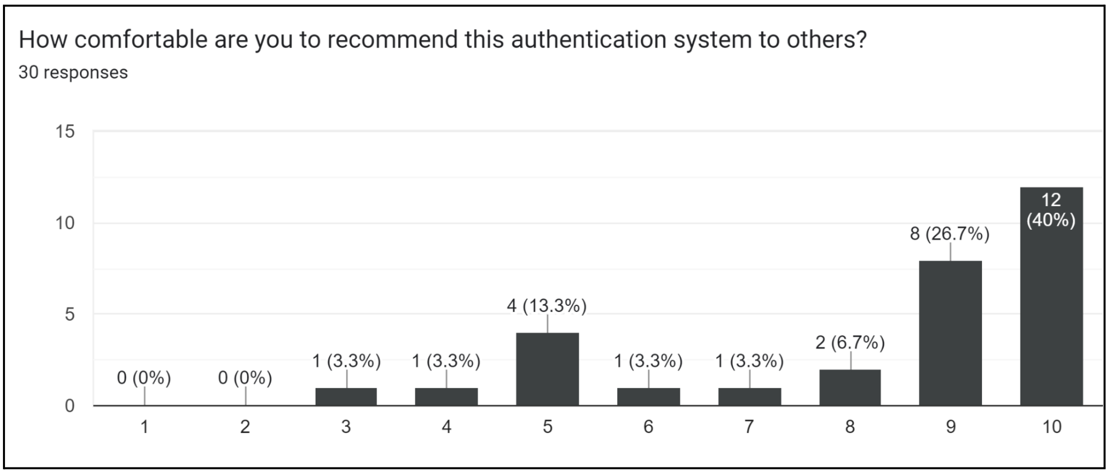


Figure 4.1. 5: Recommendation of the Authentication System [1:Not Comfortable, 10:Highly Comfortable]

With all of them have agreeing that this Authentication System would protect them better than the existing methods, they still had to face some complexity while using the Authentication System, since that we can see that the rate of recommending the system has had some ups and downs; but as an overall, since most of them are comfortable with recommending this Authentication System to their friends and colleague, this can be considered as a success.

Question: Would you like to provide any additional feedback/comments that can be used for further improvements of this system?

Finally, the responders were asked to provide additional feedback and comments from their perspective on who they think of this system; and how it can be improved for the better future. Following table contains some of the feedbacks that were provided with the responders age range;

Age Range	Provided Response
26 - 35	Being a working professional, time is precious and security is important. This system adds an extra layer of security even if it takes a bit more time.
36 - 45	I appreciate the convenience of this authentication system and how it can improve my online security.
Below 16	I thought OTP was already cool, but this takes it to the next level. I feel like I'm using secret codes to unlock things!
Above 55	Was complex for me to find all the required keys
Above 55	I can see the benefits of this system, and it's a step in the right direction. However, I did encounter some challenges due to my age.
Below 16	I think this system is pretty cool, but sometimes I have trouble remembering the codes.
16 - 25	The user experience is spot-on. I appreciate how it keeps my online

	interactions safe without being complicated.
16 - 25	As someone who values security, I'm all for this system. It's a great way to ensure my accounts are well-guarded.
26 - 35	It's nice to see systems evolving to match our security needs. This one's a winner
36 - 45	It take a bit amount of time to get into the system with this authentication system, but it provide a better security on the system. So, all in all, I'd say this is a good implementation done.

Table 4.1. 2: Additional Feedback/Comments about the System

[Please refer to ‘Appendices B: Feedbacks from Beta Test’ for further details about the above-mentioned research.]

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 '2.1. Authentication System Overview', we have discussed the in depth overview of the Authentication System and how it should work; and when we moved into the segment of '2.2. Research: Implementation of an Authentication System', we saw how the based requirements and initial plans had to be changed due to the collaborative research that was conducted by myself and Ms. M. W. N. L. De Silva.

During the segment of '3.1. System Implementations', we discussed how the system was implemented, what technologies were used, about the timelines of the Authentication System throughout the year (Gantt Charts). Moving to the segment of '3.2. 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 beta test was conducted to see the system funutilities in play with real end users to see how effective this provided Authentication System would be and how efficient this Authentication System performs. With the results that were gathered and discussed during the segment of '4.1. Results from the Beta Test', 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 Authentication System, it would be that the newly proposed and implemented Authentication System was a success.

4.3. Future Developments & Implementations

Looking forward, the advancement of the Authentication System lays areas of strength for likely upgrades and progressions. In a steadily advancing mechanical scene and with changing client requests, a few roads arise to improve security and client experience.

One way includes growing the multi-factor authentication (MFA) system. While the ongoing framework uses two-factor verification (2FA), the expansion of additional elements could additionally support security. With the collected details of the collaborative research, this system can adapt to a MFA system in the upcoming future since the people of Sri Lanka would be more adaptable and capable. This could incorporate coordinating biometric components like fingerprints or voice acknowledgment, giving an extra layer of uniqueness past conventional passwords.

One more road is the production of a devoted mobile application. This application could solidify validation systems, including the generation of OTP codes and biometric checks. Furthermore, ongoing warnings for account exercises could upgrade client mindfulness and command over their validation. With the future of Sri Lanka being more technologically advanced and the younger generations are into more Information Technology related stuff, these implementations would soon be required and beneficial.

The idea of risk-based verification presents a unique layer of safety. The framework assesses login endeavors in view of possible dangers, applying stricter confirmation for high-risk situations and smoother access for lower-risk circumstances. This approach adjusts to the constantly changing danger scene.

In this dynamic landscape, it's vital to strike a balance between security, usability, and emerging technologies. Keeping a watchful eye on evolving trends and staying informed about emerging threats will guide the ongoing development of the Authentication System.

5. CONCLUSION

Our excursion through the convergence of innovation, security, and cultural advancement has driven us to a surprising end. This quest for a Blockchain-Based Criminal Data The board Framework, especially the imaginative Confirmation Framework, goes past simple scholastic investigation. It features the powerful transaction among advancement and the necessities of our general public.

This exploration began by unraveling the intricacies of managing criminal information and the vulnerabilities that demand protection. The Authentication System we've developed isn't just another solution—it's a fusion of traditional and futuristic elements. It blends familiar username-password combinations with cutting-edge one time password (OTP) generations and verification checks. This balance, struck between robust security and user convenience, emerged as we fortified layers of defense and put them to the test.

The Beta Test phases were pivotal moments, highlighting the dedication invested in this endeavor. The results showcased in the End Results segment testified to the transformation achieved—an authentication ecosystem that's adaptable, responsive, and aligned with the aspirations of our digitally-driven society. Our journey evolved from 6-digit OTP codes to fortified 6-character codes, from well-established approaches to visionary innovations. This voyage exemplifies how innovation takes shape through evolution.

Looking ahead, this thesis contributes not just to our understanding of authentication systems, but also opens doors for further exploration. The future gleams with opportunities—integrating blockchain's unchangeable security, expanding biometric factors, or embracing adaptive authentication that adjusts to changing user behaviors.

A vital lesson we've learned is that innovation knows no bounds. It bridges the gap between theories and practical applications, making dreams tangible. As we conclude, it's clear that knowledge isn't static; it grows with time, context, and technological progress. We're reminded to harness innovation to shape secure futures, where technology and security coexist to nurture a safer, more connected society.

In essence, this thesis celebrates our accomplishments, but it's also a call to embrace the uncharted realm of technological evolution and unwavering security. Our journey thus far is an exploration of connecting understanding with action, fusing theory with real-world impact. As we look ahead, the Authentication System stands as proof of potential unlocked through innovation—a symbol of the resilient spirit that drives progress toward a safer world.

As we conclude this journey, the Authentication System stands not just as an accomplishment, but as a symbol of progress. In a world where our digital society relies on data, this system represents our commitment to using innovation for the greater good. It shows that we can enhance security without sacrificing user experience, creating a stronger future. This ending isn't a finish line, but a testament to our ability to find solutions that shape the world we want. The impact of this effort goes beyond these pages, encouraging us to keep exploring, driving change, and embracing the endless possibilities of innovation in the unknown paths ahead.

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] E. Huseynov and J.-M. Seigneur, "WiFiOTP: Pervasive two-factor authentication using Wi-Fi SSID broadcasts," in IUT Kaleidoscope International Conference, Barcelona, Spain, 2015, doi: 10.1109/Kaleidoscope.2015.7383630.

[8] "What Is Multi-Factor Authentication (MFA)?," Amazon Web Services, Inc, [Online]. Available: https://aws.amazon.com/what-is/mfa/. [Accessed 20 March 2023].

[9] L. Rosencrance, P. Loshin and M. Cobb, "Two-factor authentication (2FA)," TechTarget, July 2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/two-factor-authentication. [Accessed 21 March 2023].

[10] G. Orenstein, "3 tips from NIST to keep your passwords secure," Bitwarden, 11 August 2022. [Online]. Available: https://bitwarden.com/blog/3-tips-from-nist-to- keep-passwords-secure/. [Accessed 22 March 2023]

[11] G. Orenstein, "How long should my password be? Make your password 14 to 16 characters or more!," Bitwarden, 11 October 2022. [Online]. Available: 11. https://www.mcafee.com/learn/how-often-should-you-change-your-passwords/#:~:text=Cybersecurity%20experts%20recommend%20changing%20your,has%20access%20to%20your%20account.. [Accessed 22 March 2023]

[12] "IBM Security Privileged Identity Manager 2.0.0," IBM Corporation, 08 March 2021. [Online]. Available: https://www.ibm.com/docs/en/spim/2.0.0?topic=administration-password-policies. [Accessed 22 March 2023].

[13] "About OpenCV," OpenCV, [Online]. Available: https://opencv.org/about. [Accessed 22 March 2023].

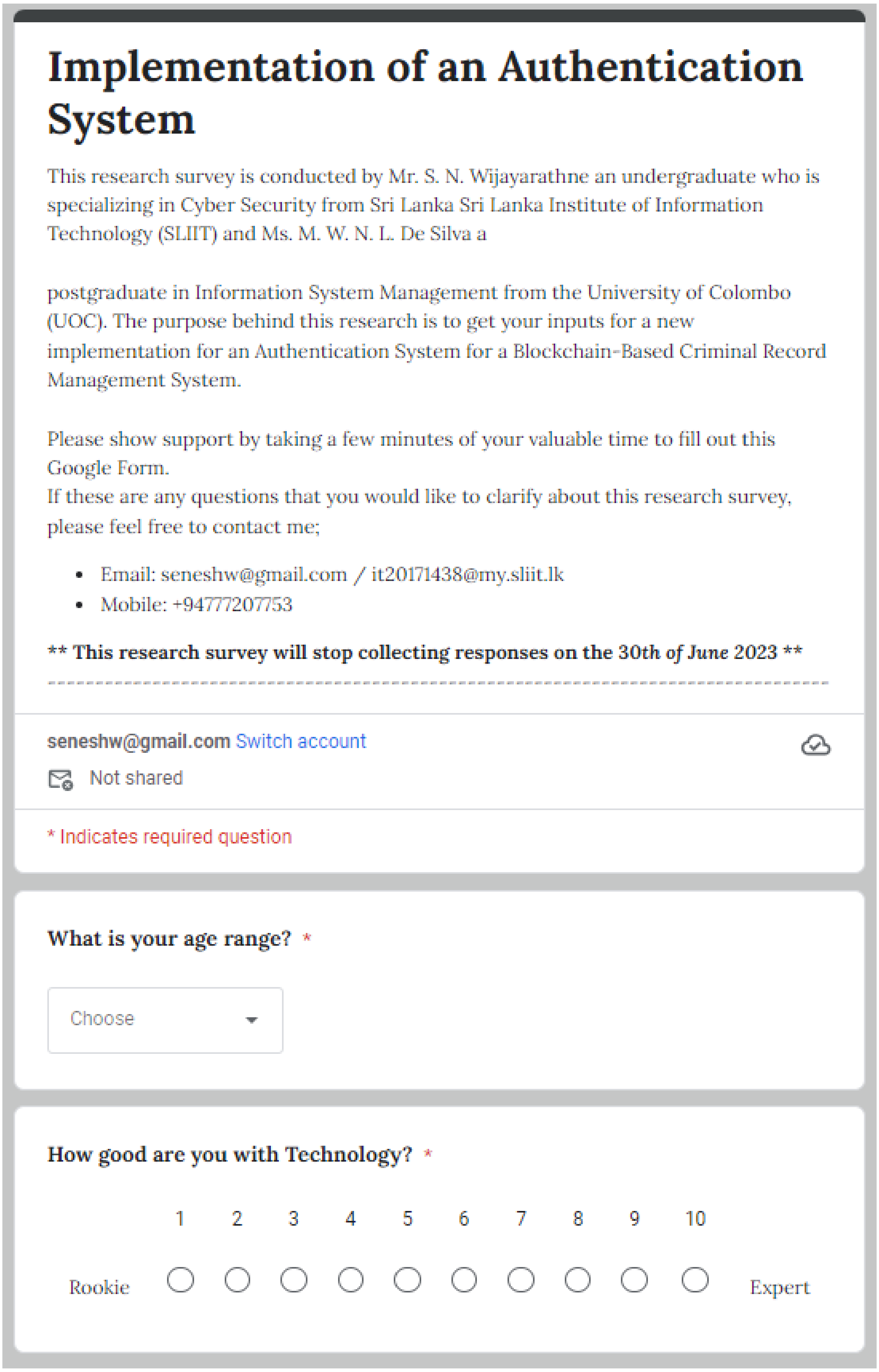
[14] "HMAC (Hash-Based Message Authentication Codes) Definition," Okta, 14 February 2023. [Online]. Available: https://www.okta.com/identity-101/hmac/#:~:text=Hash%2Dbased%20message%20authentication%20code,use%20signatures%20and%20asymmetric%20cryptography.. [Accessed 22 March 2023]

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

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

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

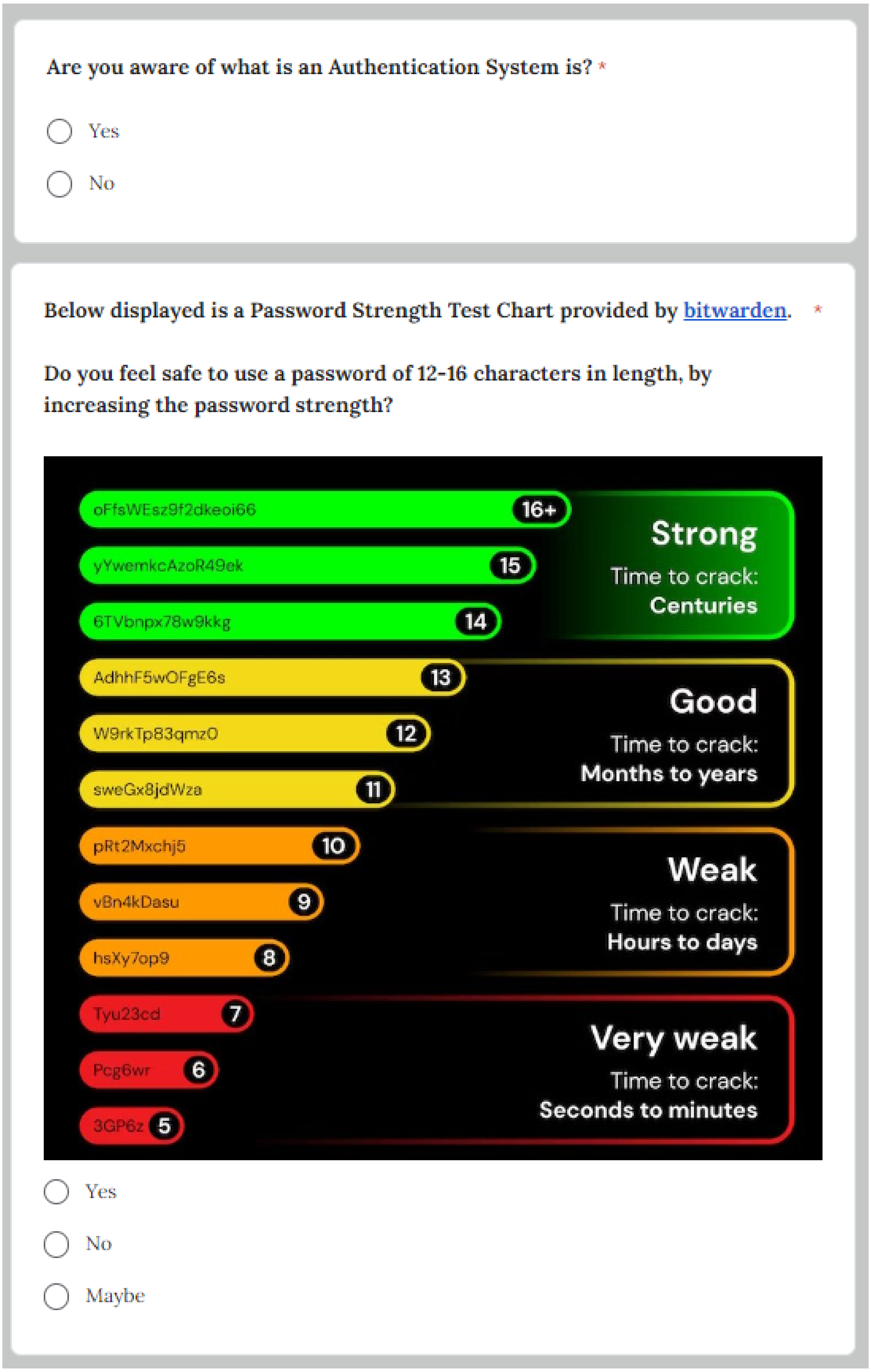
* Indicates required question

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

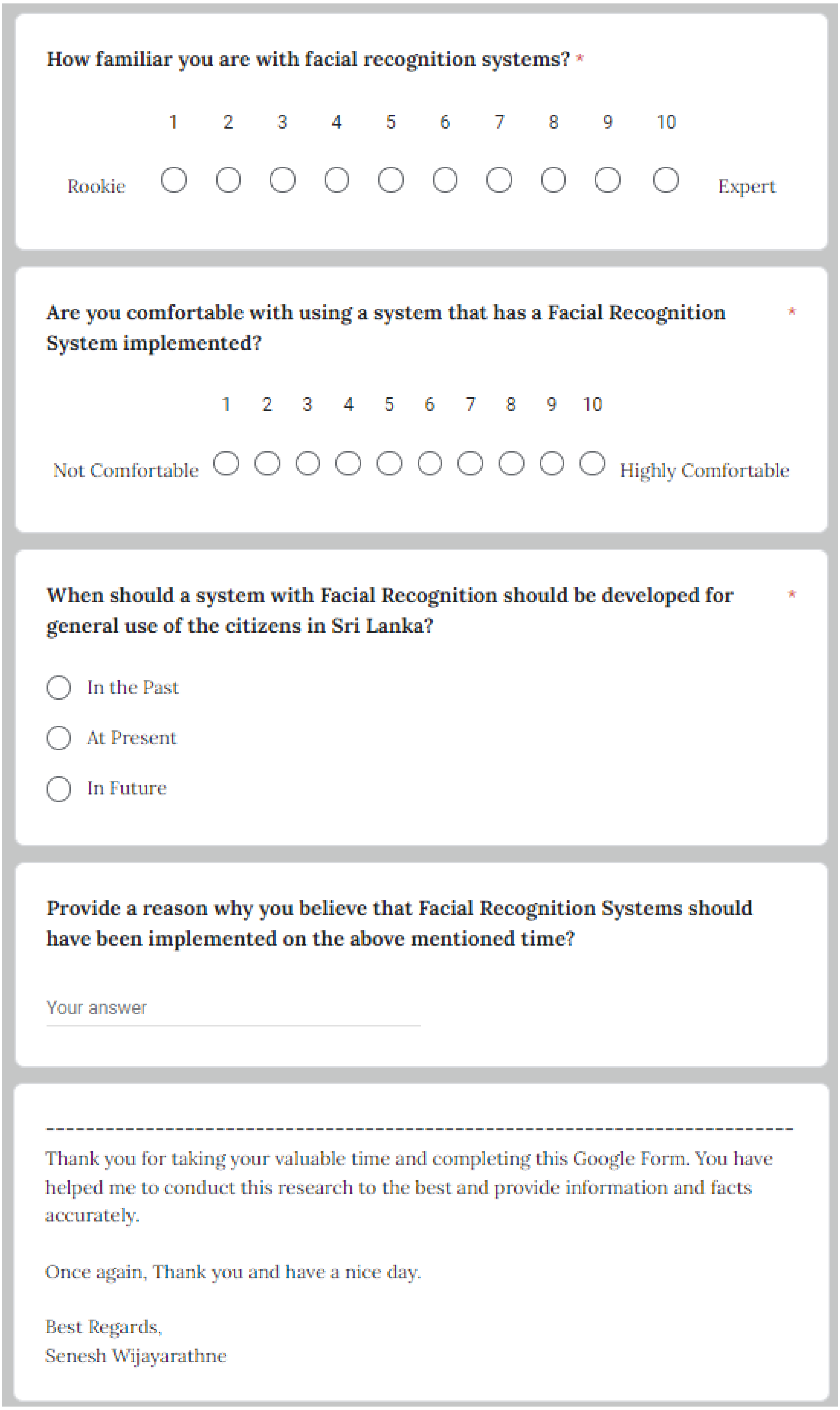
Below displayed is a Password Strength Test Chart provided by bitwarden. *

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?

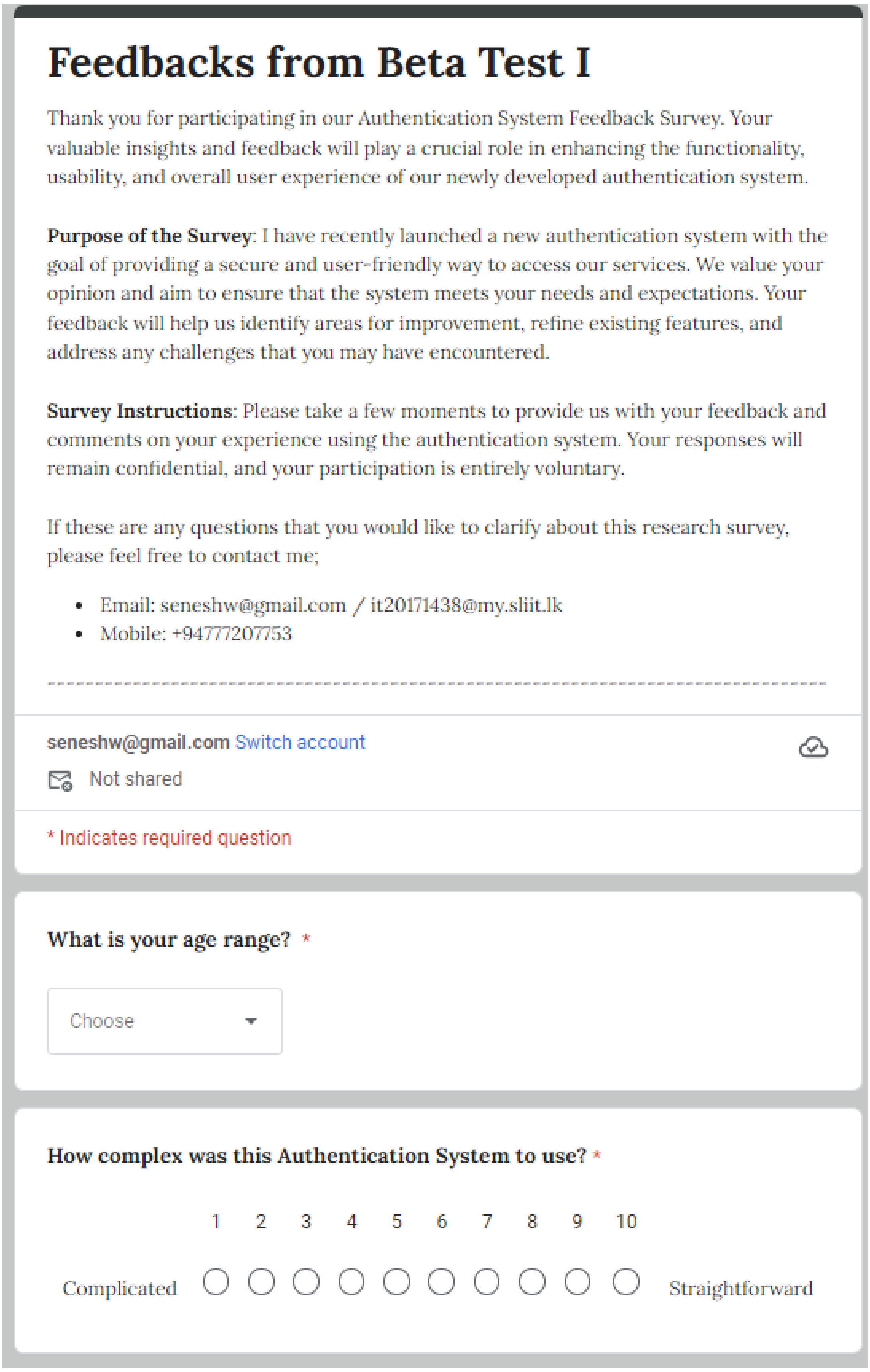
Your answer

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,
Senesh Wijayarathne

Appendices B: Feedbacks from 'Beta Test'



Feedbacks from Beta Test I

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

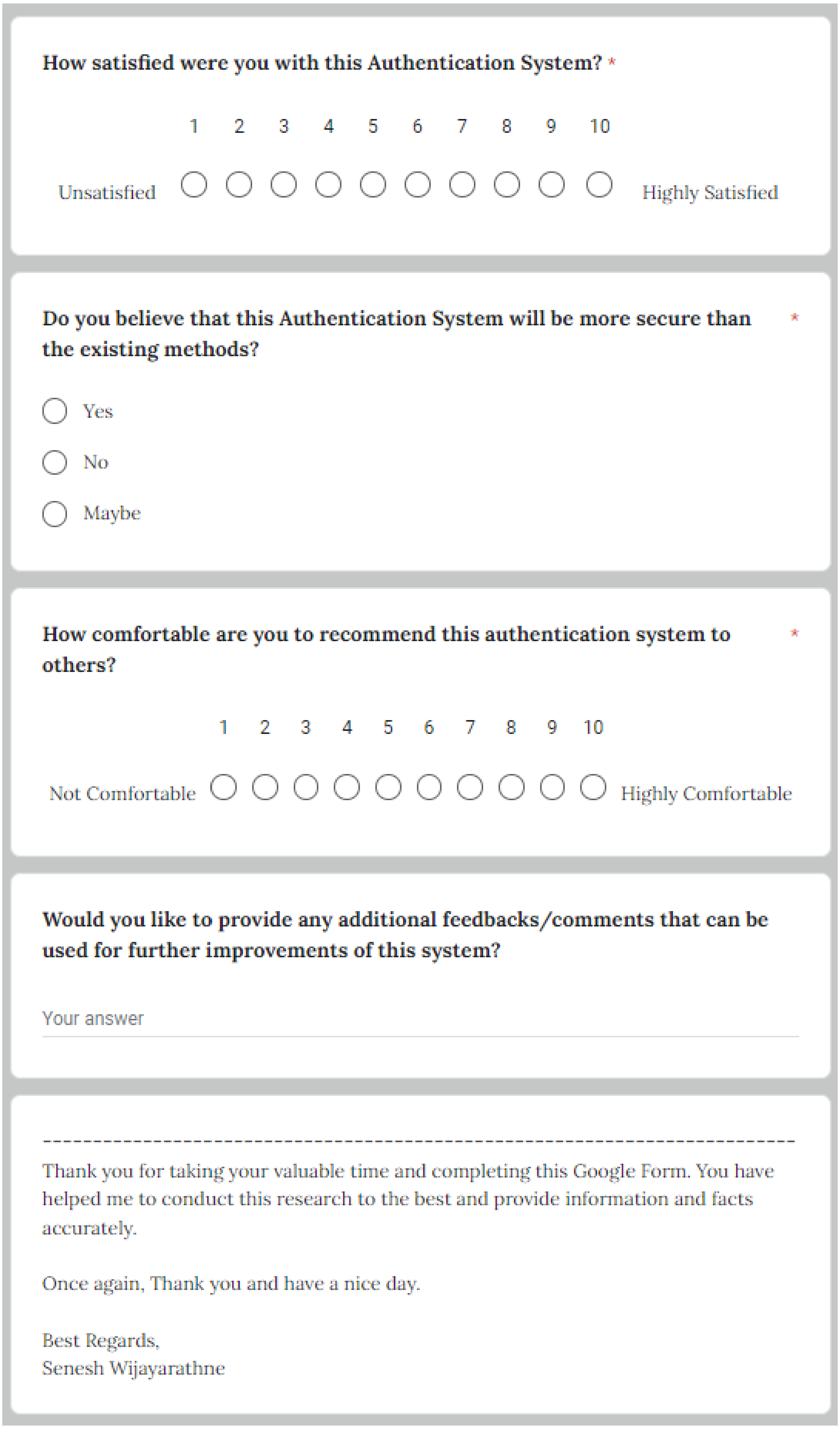
* Indicates required question

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 comfortable are you to recommend this authentication system to others? *

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

Would you like to provide any additional feedbacks/comments that can be used for further improvements of this system?

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,
Senesh Wijayarathne