SLIIT
FACULTY OF COMPUTING

BLOCKCHAIN BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA

-- GROUP ID: 23-270 --

TABLE OF CONTENT

Project Details

- Project ID: 23-270
- Supervisor: Mr. Kanishka Yapa
- Co-Supervisor: Ms. Dinithi Pandithage

GROUP MEMBERS

IT20150952
BRAHANAWARDHAN B.

IT20171438
WIJAYARATHNE S.N.

IT20157814
AHMED M.N.H.

IT19983370
THUSHITHARAN M.

CRISYS

PROJECT OVERVIEW

Blockchain Based Criminal Information Management System

The project aims to develop a blockchain-based criminal information management system as an improvement of the existing criminal information management method in Sri Lankan. This system will leverage blockchain technology to enhance data Security, transparency and efficiency in managing criminal records

- Designing Smart contract with blockchain network to ensure the CIA.
- Multi-factor Authentication.
- Developing Secure file management system for Blockchain Network.
- Develop a Chain of custody process for Criminal System.

RESEARCH QUESTION

- How can a blockchain-based criminal information management system be implemented effectively in Sri Lanka to enhance data security, transparency, and efficiency in the criminal justice system ?

  - Understand the Current Criminal System in Sri Lanka
  - Identify the Stakeholders
  - Define the System Requirements
  - Develop a Blockchain Architecture
  - Integrate with Criminal System.

RESEARCH PROBLEM

- Lack of integration
- Inconsistent data quality
- Privacy and security concern
- Insufficient process
- Lack of transparency

OBJECTIVES

01 SMART CONTRACT

Deployment of Criminal Records in blockchain

03 INTERPLANETARY FILE SYSTEM

To Secure Store criminal Evidence Document

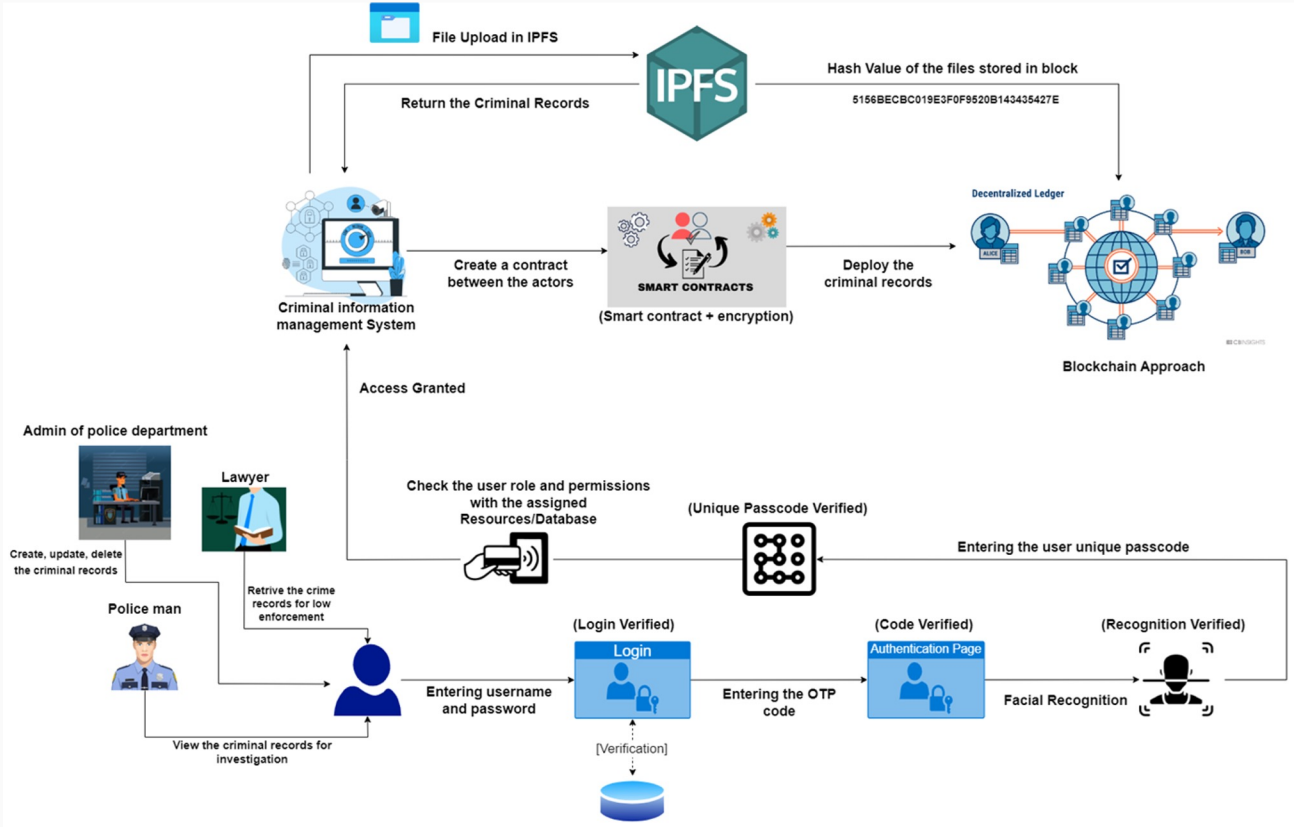
02 MULTI-FACTOR AUTHENTICATION

Prevent from the Unauthorized access

04 CHAIN OF CUSTODY

To provide a high level of security for criminal records verify the evidence

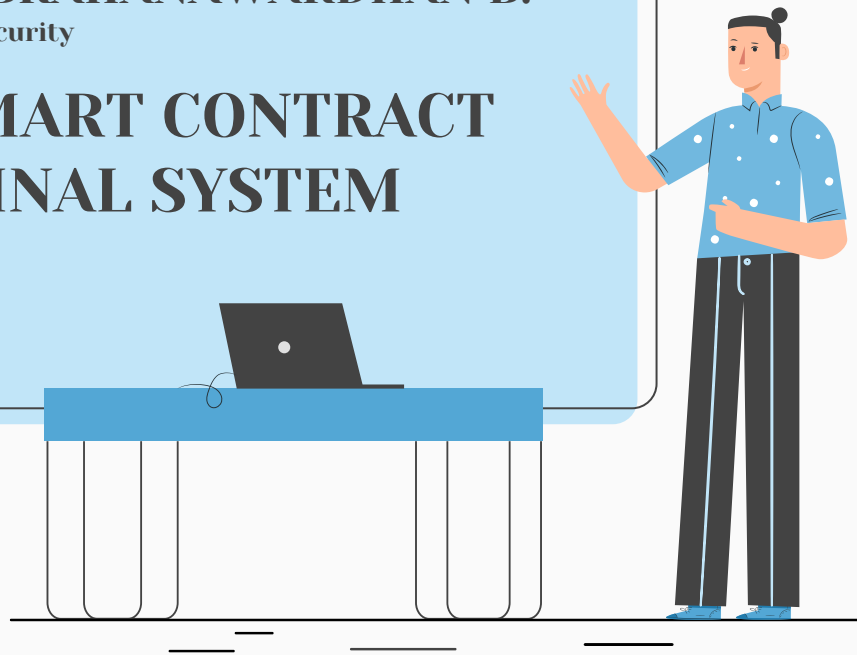
OVERALL SYSTEM DIAGRAM



IT20150952 | BRAHANAWARDHAN B.

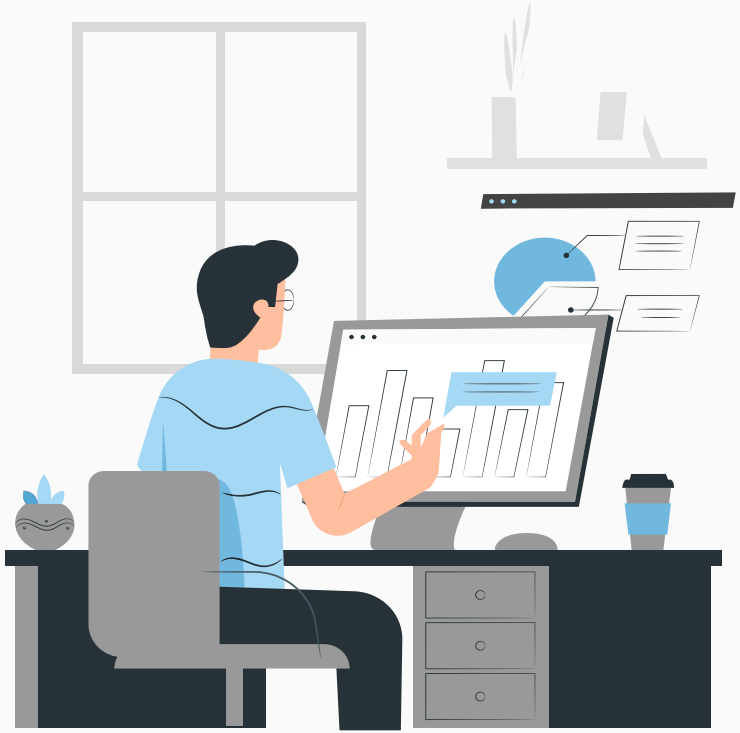
Specializing in Cyber Security

DESIGN SMART CONTRACT FOR CRIMINAL SYSTEM

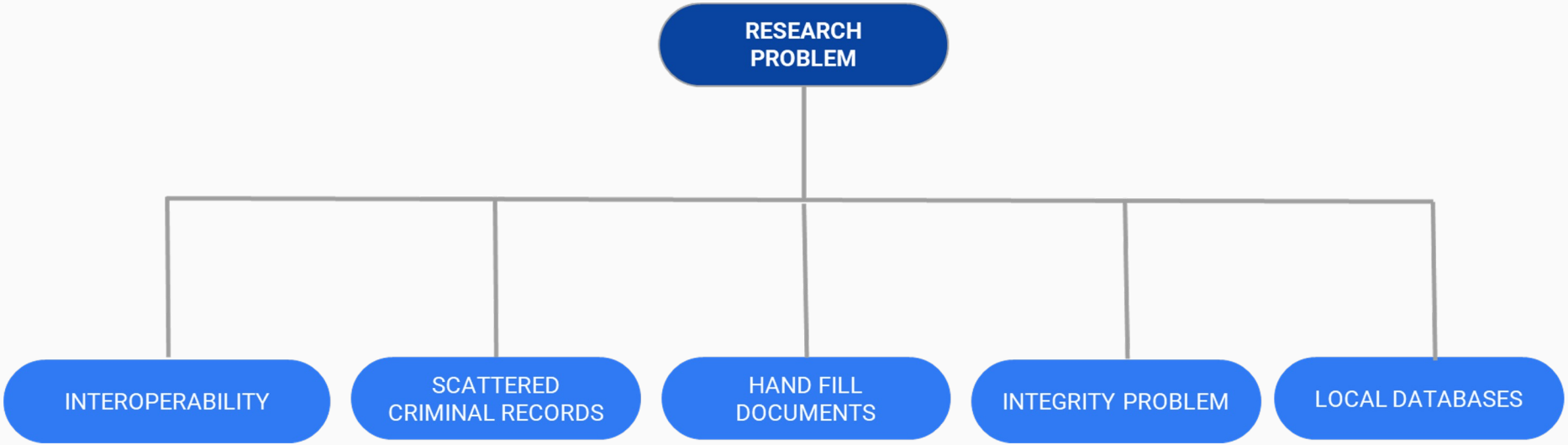


RESEARCH QUESTION

1. RESEARCH PROBLEM
2. RESEARCH GAP
3. SUB OBJECTIVES
4. REQUIREMENTS



RESEARCH PROBLEM



RESEARCH QUESTION

- How can the implementation of smart contracts in a blockchain-based criminal information management system improve the efficiency, transparency, and security of criminal investigations in sri Lanka Criminal Information Management system ?

RESEARCH GAP

CONSIDERATION ON	EXISTING LOCAL DATABASE BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA	BLOCKCHAIN TECHNOLOGY FOR CRIMINAL INFORMATION MANAGEMENT SYSTEM
Security of Sensitive Criminal Records	MEDIUM	HIGH
Decentralization Of System	LOW	HIGH
Ensure data Integrity	LOW	HIGH
Prevent loss of data	LOW	HIGH
Availability	MEDIUM	HIGH
Confidentiality	LOW	HIGH

SPECIFIC OBJECTIVES

- Increased efficiency, transparency, and security of Criminal Records.
- Ensure Confidentiality, Integrity, Availability.
- Reduce the lack of consistency.
- Increase the performance and usability of criminal Records.

SUB OBJECTIVES

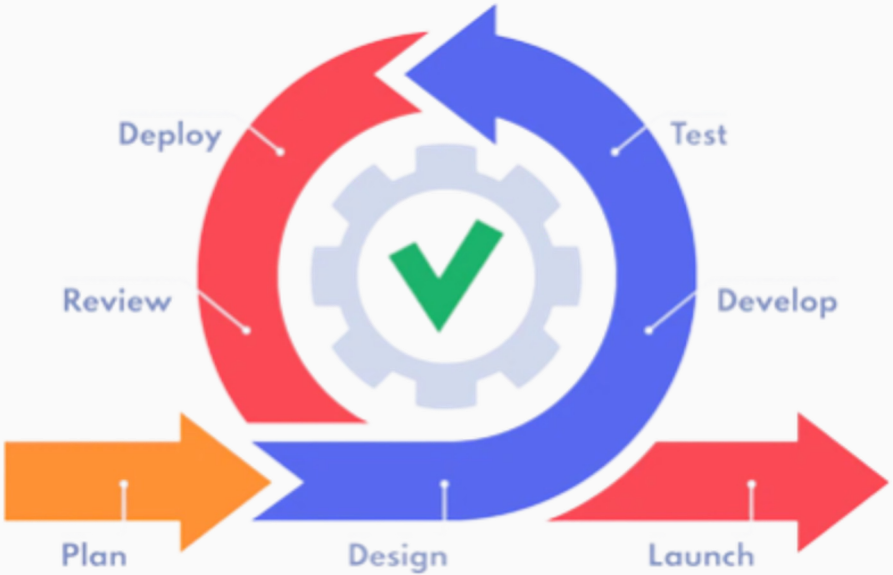
- Identify the current CIMS in Sri Lanka and limitation.
- Review the literature on smart contracts.
- Conduct a feasibility study
- Identify the stakeholders
- Develop a prototype
- Recommendations and guidelines

METHODOLOGY

Data Collections and understand the current criminal records handling method in Sri Lanka

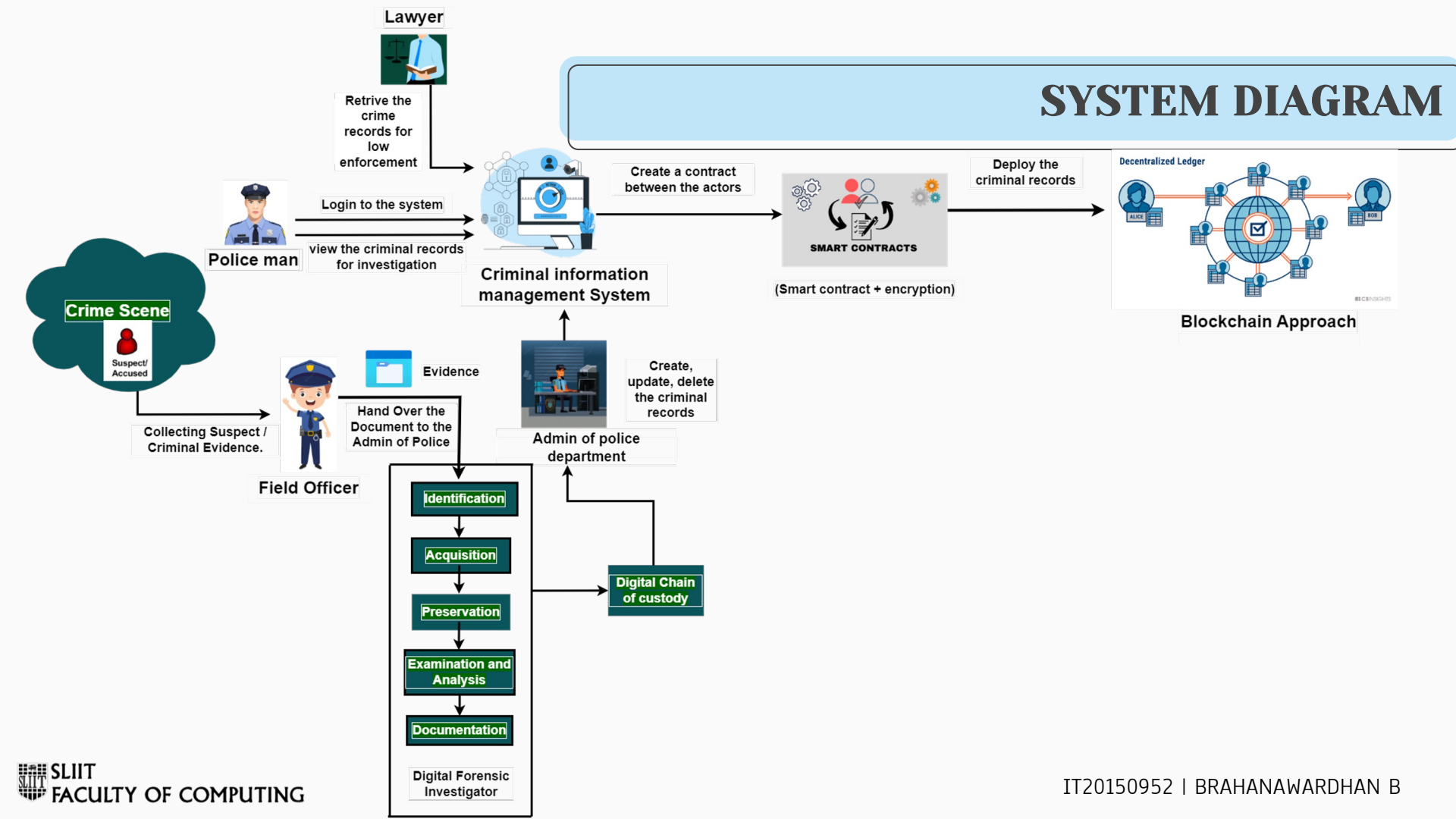
- Feasibility Study on Blockchain Network.
- Design Smart contract for Blockchain.
- Implementing Criminal System.

DEVELOPMENT CYCLE



- Why 'The Agile Life Cycle" was used?
  - Flexibility
  - Iterative Approach
  - Collaboration & Communication
  - Continuous Improvement
  - Rapid Prototyping
  - Time & Resource Management

SYSTEM DIAGRAM



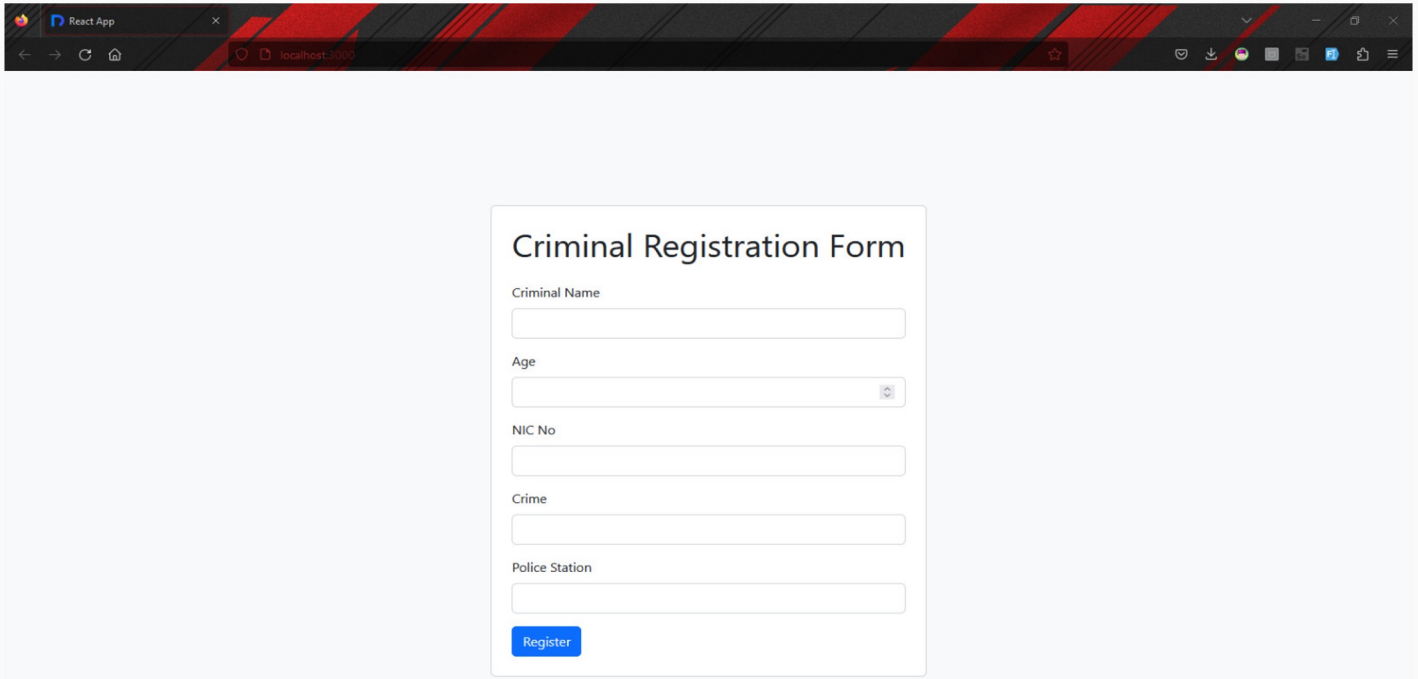
FUNCTIONAL REQUIREMENTS

- Criminal Records Data Entry
- Criminal Records Data Search
- Data Privacy and Security
- Immutable Criminal Records Keeping
- Integration with Criminal System.

NON – FUNCTIONAL REQUIREMENTS

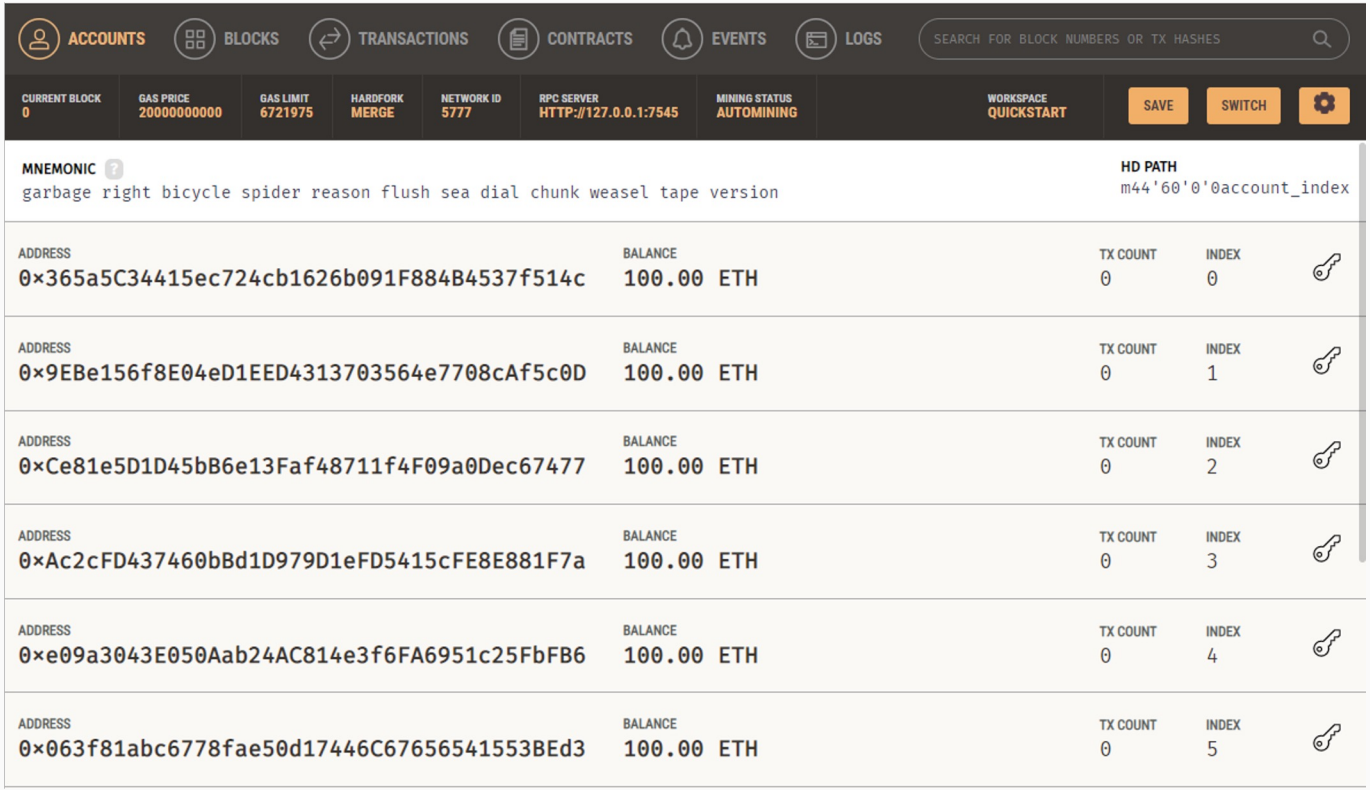
- Scalability of the Blockchain
- Reliability and Availability of Data.
- Interoperability
- Compliance
- Usability
- Performance

Criminal Data Entry web page

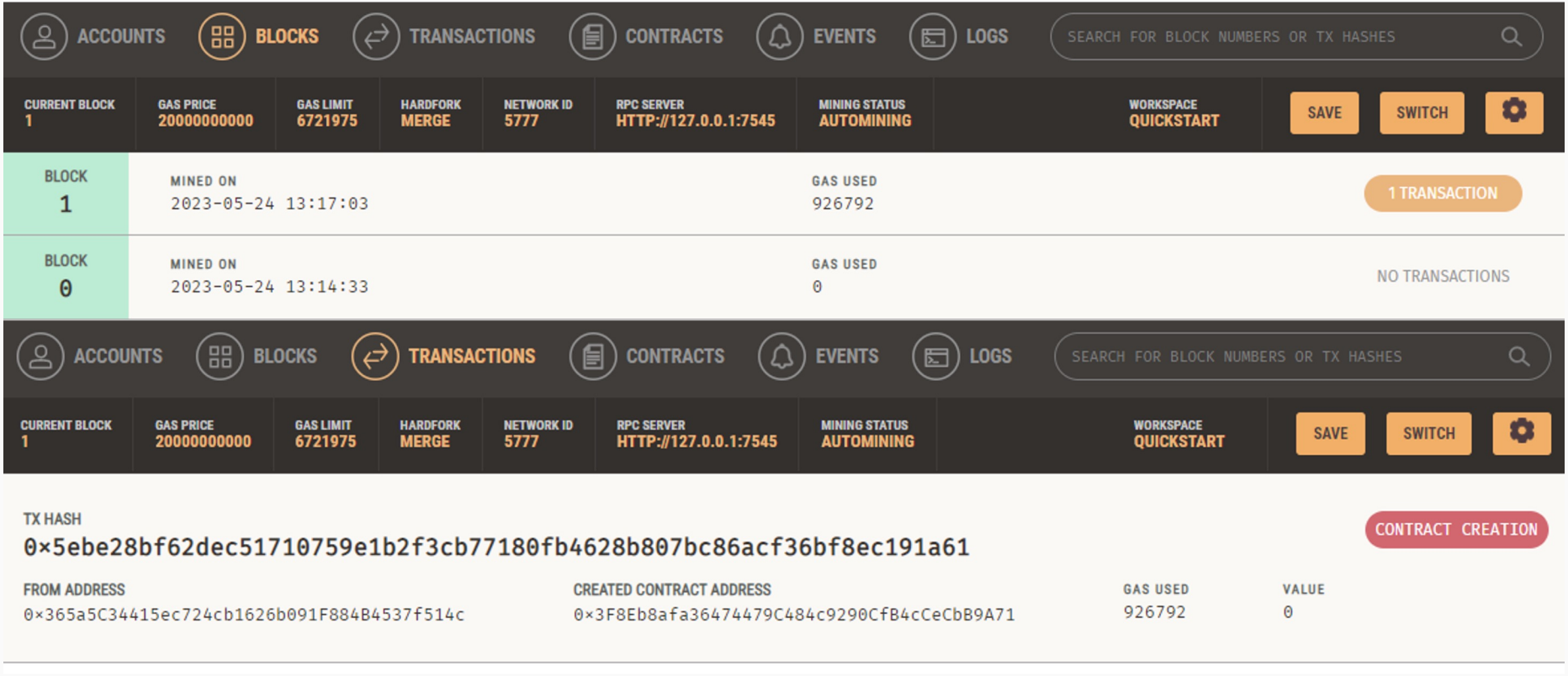


IMPLEMENTATIO N

Ganache Blockchain for Criminal Information Management System

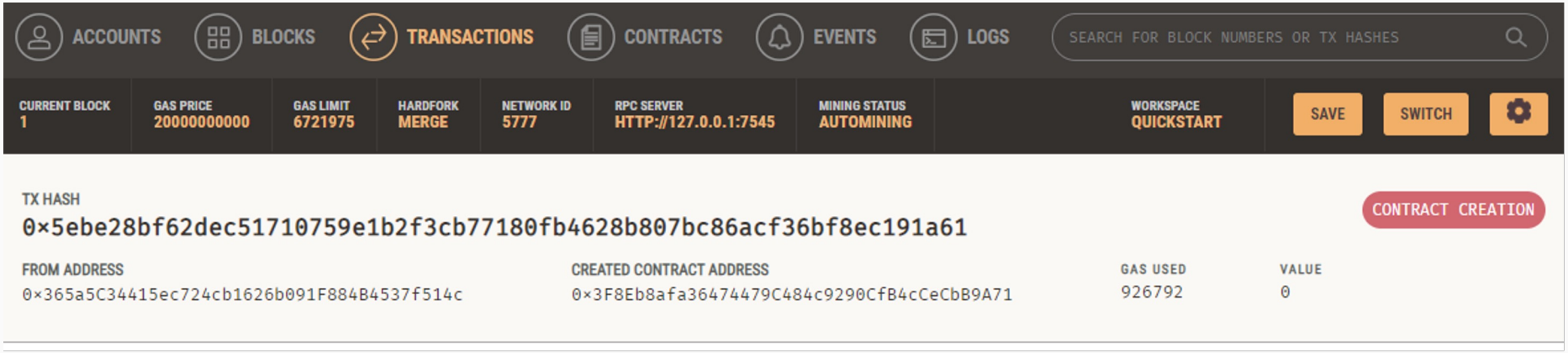


Ganache Blockchain for Criminal Information Management System



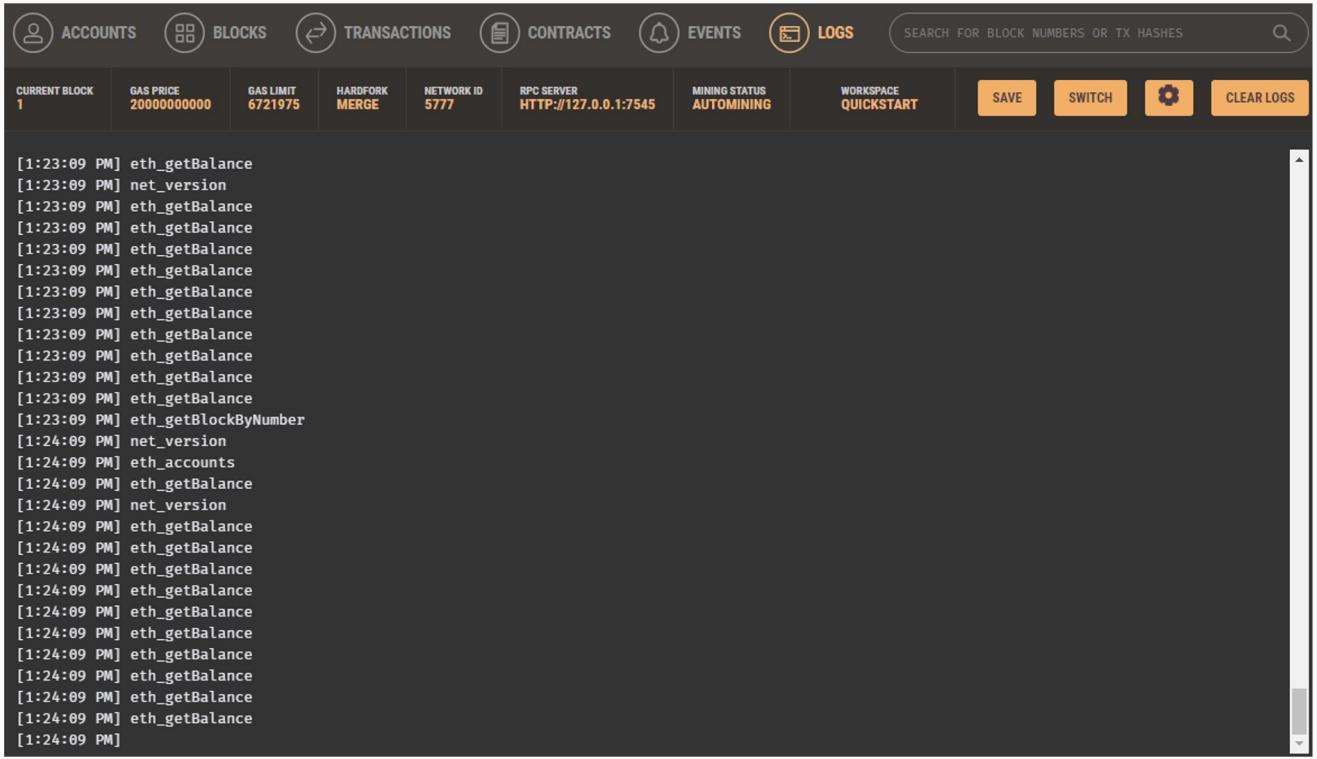
Ganache Blockchain for Criminal Information Management System

- **Initial Transaction**

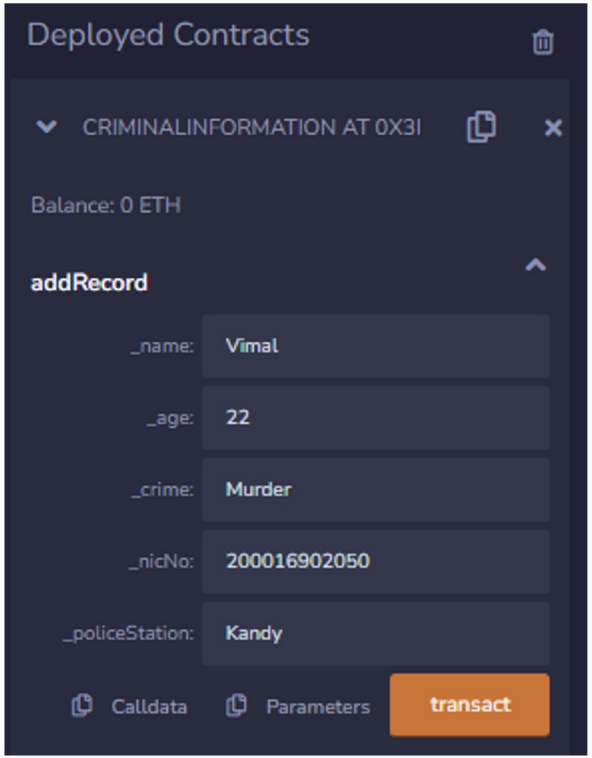


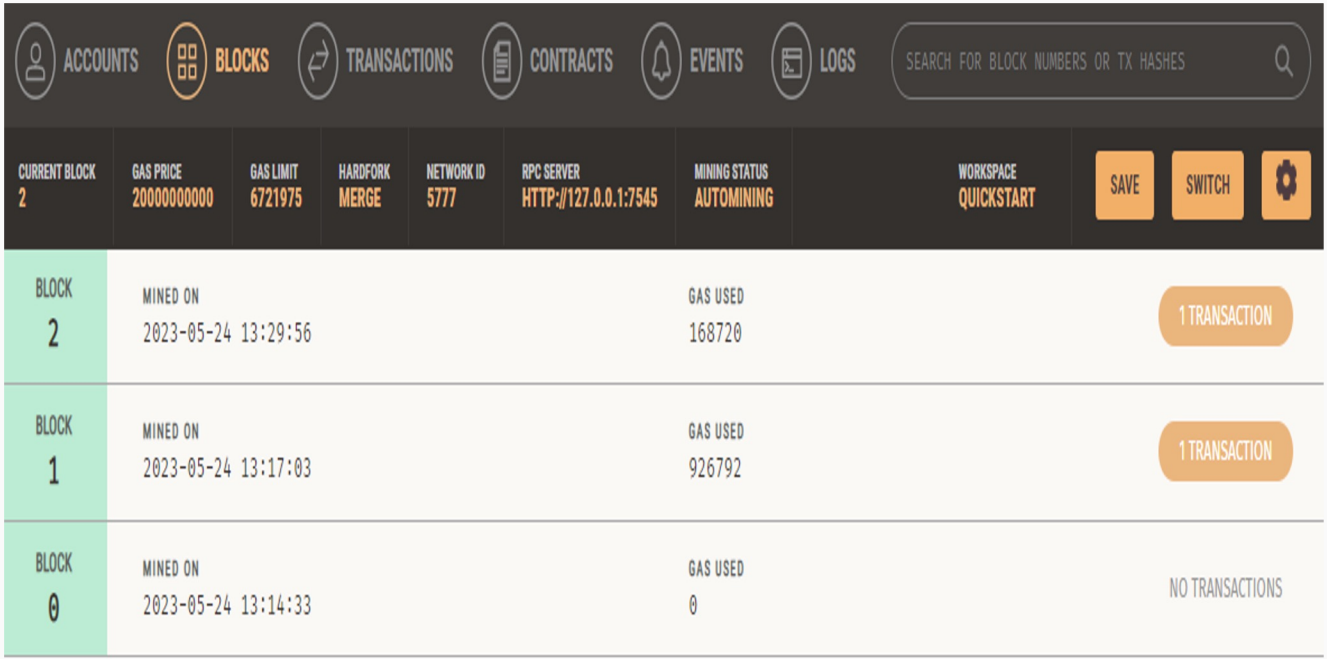
Ganache Blockchain for Criminal Information Management System

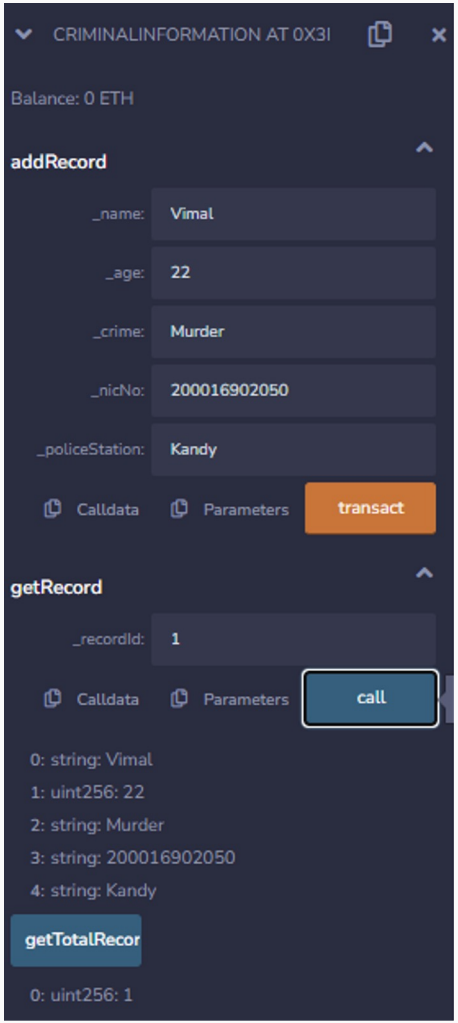
- **Record All logs from the transaction**

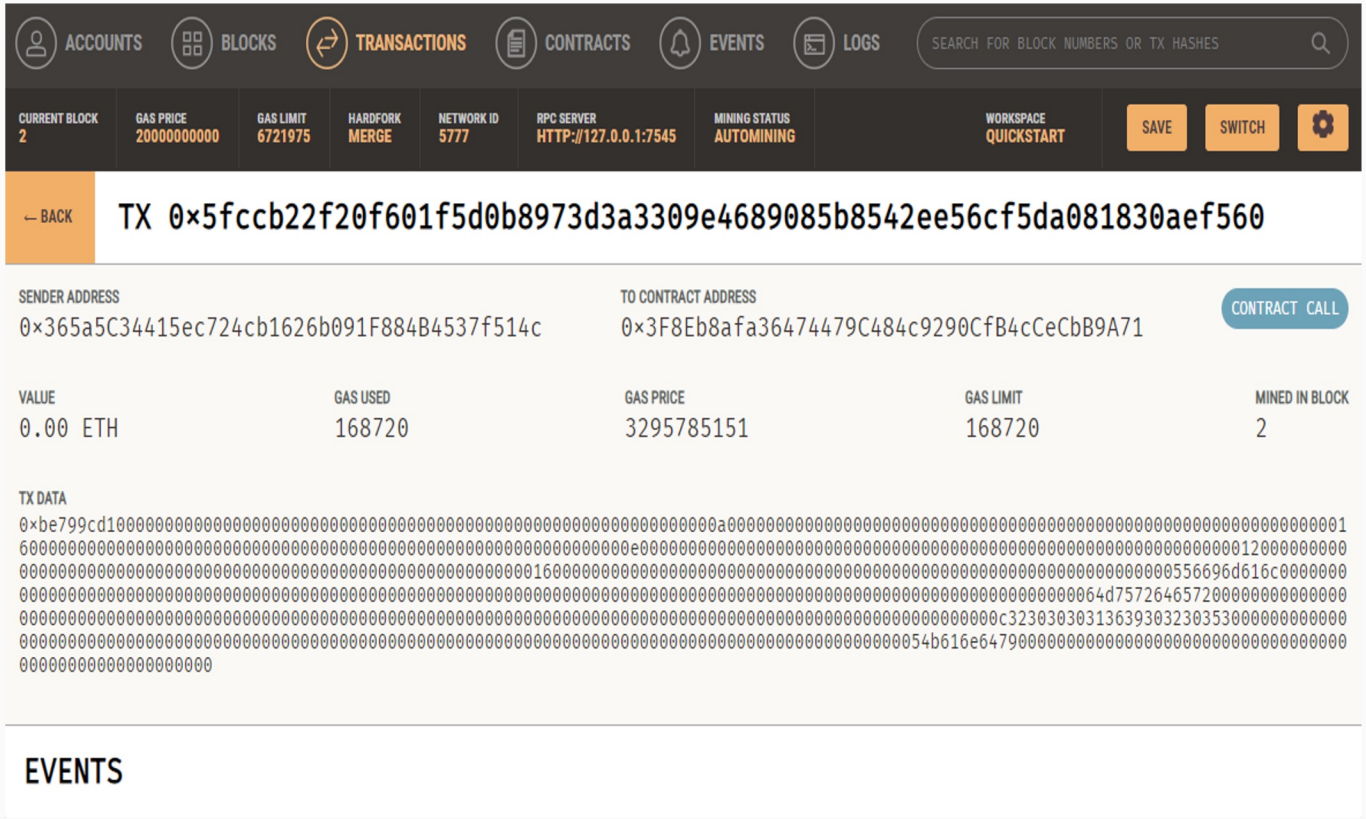


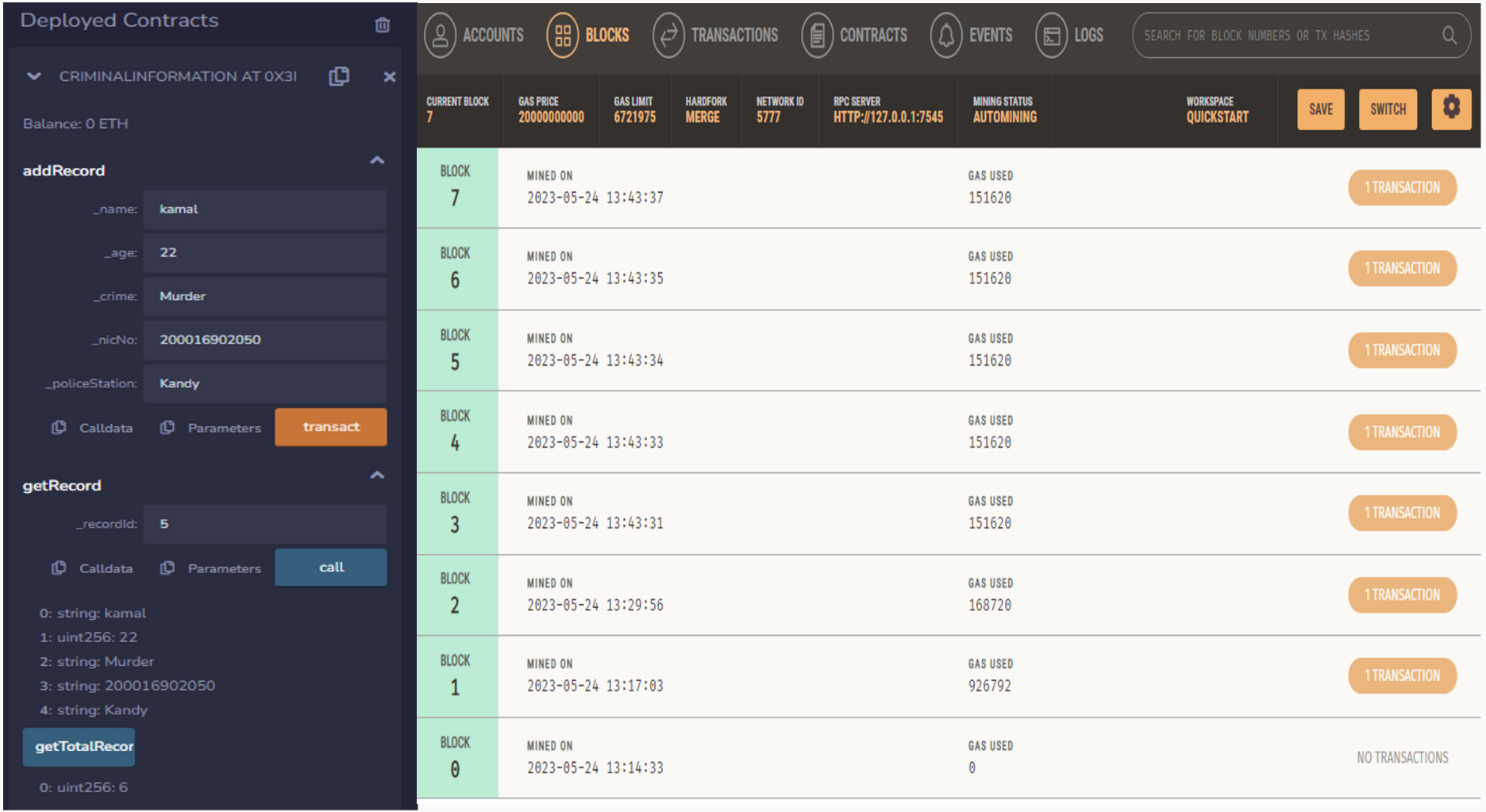
Working Functionality for Criminal Records – Input the Records



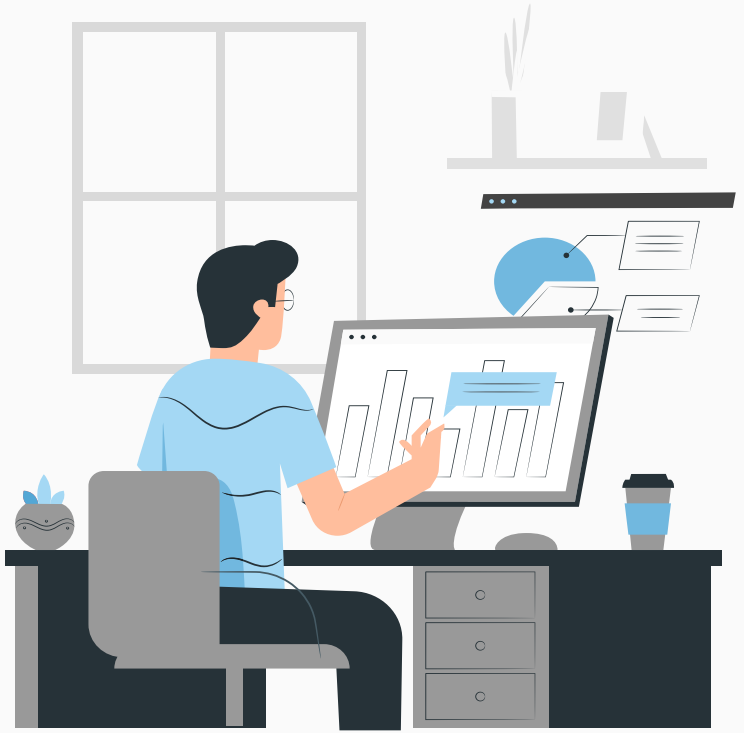



CRIMINALINFORMATION AT 0X3I
Balance: 0 ETH
addRecord
_name: Vimal
_age: 22
_crime: Murder
_nicNo: 200016902050
_policeStation: Kandy
Calldata
Parameters
transact
getRecord
_recordId: 1
Calldata
Parameters
call
0: string: Vimal
1: uint256: 22
2: string: Murder
3: string: 200016902050
4: string: Kandy
getTotalRecor
0: uint256: 1


ACCOUNTS
BLOCKS
TRANSACTIONS
CONTRACTS
EVENTS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 2
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MERGE
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE QUICKSTART
SAVE
SWITCH
← BACK
TX 0×5fccb22f20f601f5d0b8973d3a3309e4689085b8542ee56cf5da081830aef560
SENDER ADDRESS
0×365a5C34415ec724cb1626b091F884B4537f514c
TO CONTRACT ADDRESS
0×3F8Eb8afa36474479C484c9290CfB4cCeCbB9A71
CONTRACT CALL
VALUE
0.00 ETH
GAS USED
168720
GAS PRICE
3295785151
GAS LIMIT
168720
MINED IN BLOCK
2
TX DATA
0×be799cd1000000000000000000000000000000000000000000000000000000000000000a0000000000000000000000000000000000000000000000000000000000000001
6000000000000000000000000000000000000000000000000000000000000000e0000000000000000000000000000000000000000000000000000000000000012000000000
0000000000000000000000000000000000000000000000000000000000000016000000000000000000000000000000000000000000000000000000000556696d616c0000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000064d7572646572000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000c323030303136393032303530000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000054b616e6479000000000000000000000000000000000
0000000000000000000
EVENTS

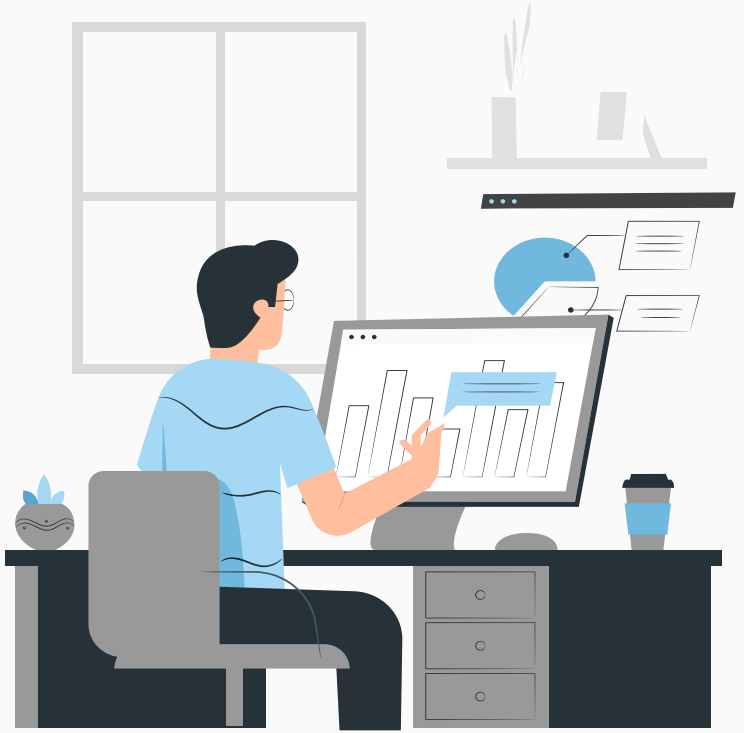

Deployed Contracts
CRIMINALINFORMATION AT 0X3I
Balance: 0 ETH
addRecord
_name: kamal
_age: 22
_crime: Murder
_nicNo: 200016902050
_policeStation: Kandy
Calldata
Parameters
transact
getRecord
_recordId: 5
Calldata
Parameters
call
0: string: kamal
1: uint256: 22
2: string: Murder
3: string: 200016902050
4: string: Kandy
getTotalRecor
0: uint256: 6
ACCOUNTS
BLOCKS
TRANSACTIONS
CONTRACTS
EVENTS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 7
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MERGE
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE QUICKSTART
SAVE
SWITCH
BLOCK 7 MINED ON 2023-05-24 13:43:37 GAS USED 151620 1 TRANSACTION
BLOCK 6 MINED ON 2023-05-24 13:43:35 GAS USED 151620 1 TRANSACTION
BLOCK 5 MINED ON 2023-05-24 13:43:34 GAS USED 151620 1 TRANSACTION
BLOCK 4 MINED ON 2023-05-24 13:43:33 GAS USED 151620 1 TRANSACTION
BLOCK 3 MINED ON 2023-05-24 13:43:31 GAS USED 151620 1 TRANSACTION
BLOCK 2 MINED ON 2023-05-24 13:29:56 GAS USED 168720 1 TRANSACTION
BLOCK 1 MINED ON 2023-05-24 13:17:03 GAS USED 926792 1 TRANSACTION
BLOCK 0 MINED ON 2023-05-24 13:14:33 GAS USED 0 NO TRANSACTIONS

Demonstration



PENDING WORK

- Update Smart Contract and Integration
- Integration with Criminal System.

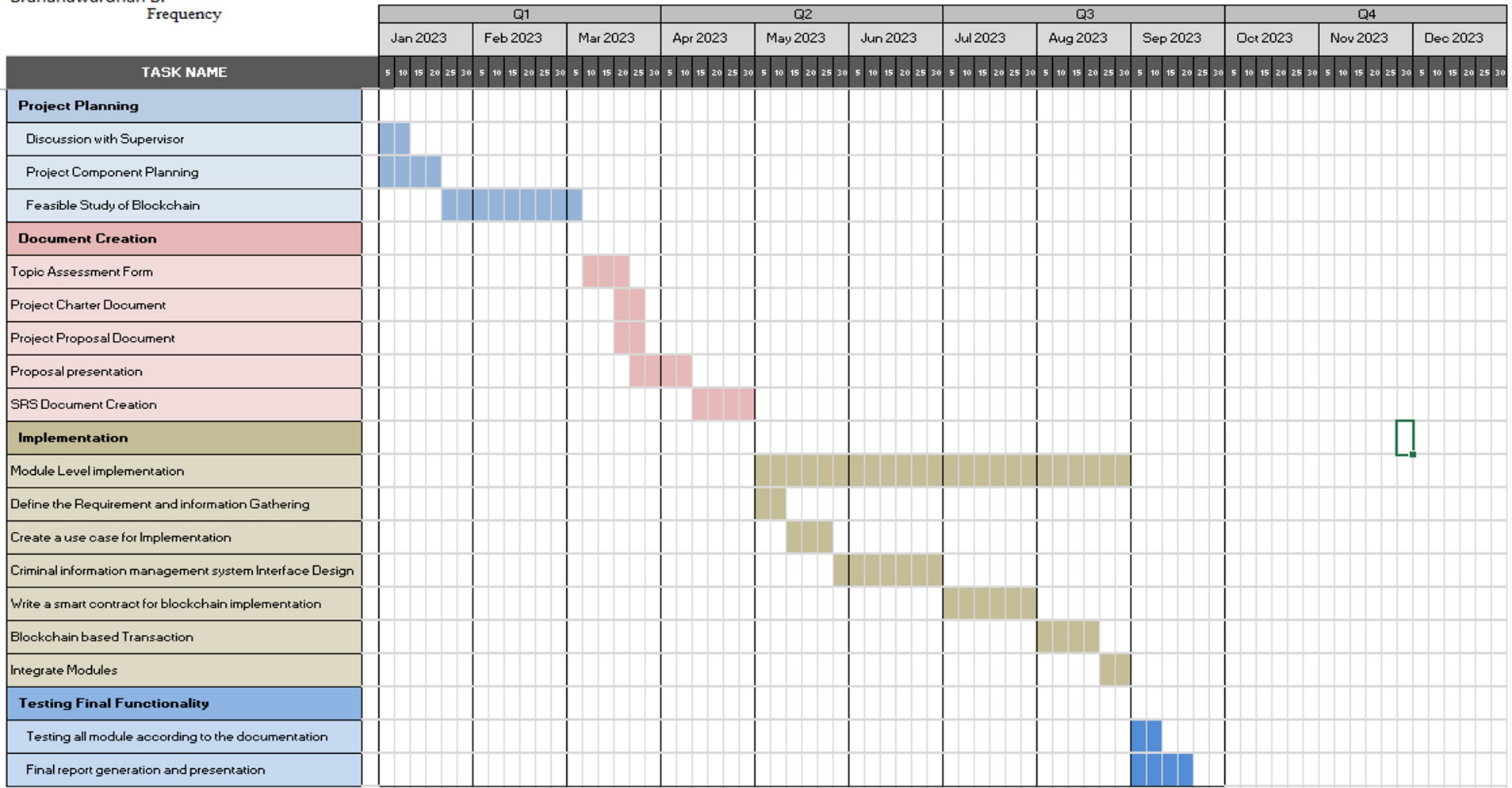


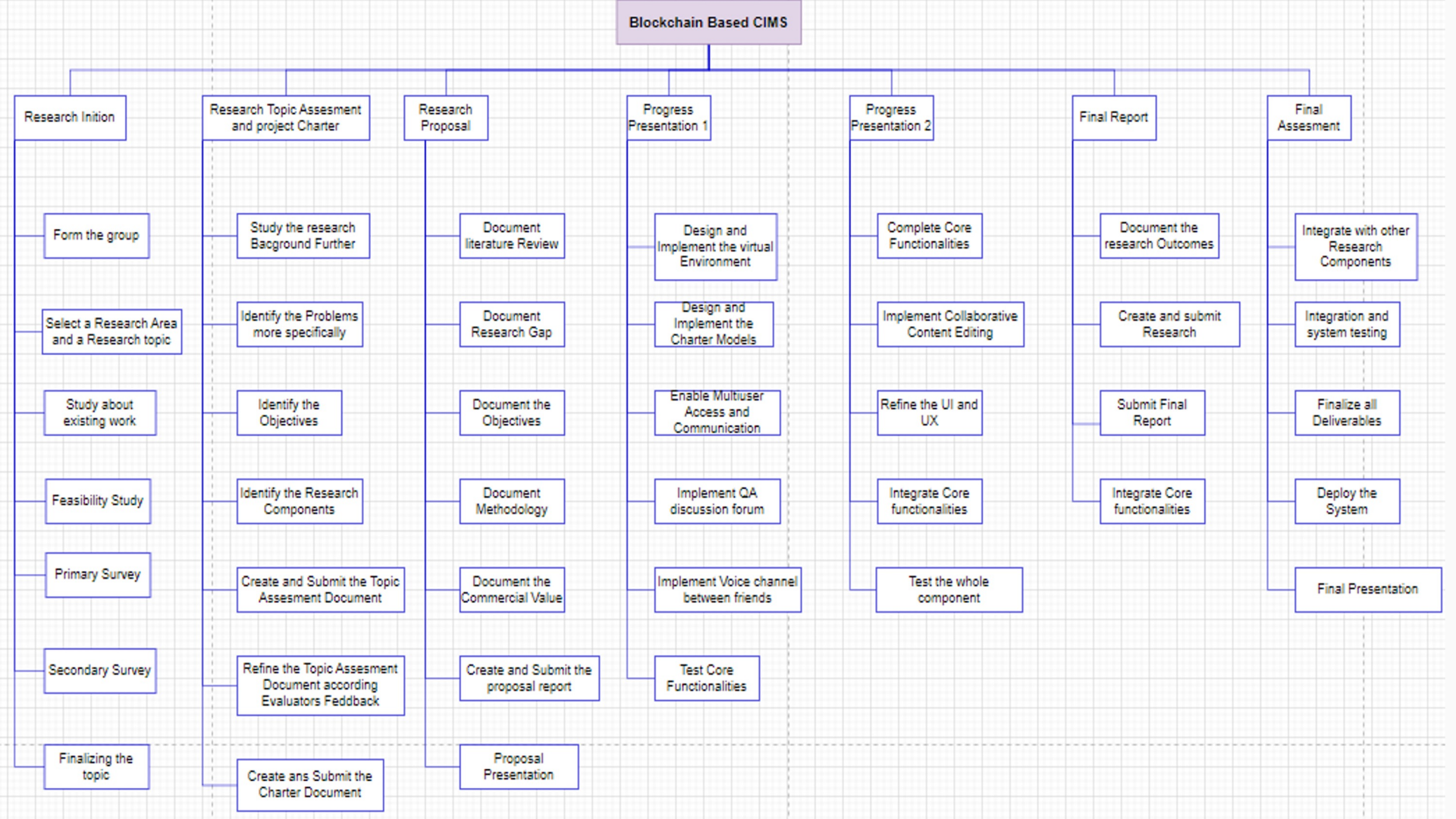
Research Project - Timeline

Sri Lanka Institute of Information Technology (SLIIT)

Brahanawardhan B.

Frequency




Blockchain Based CIMS
Research Inition
Form the group
Select a Research Area and a Research topic
Study about existing work
Feasibility Study
Primary Survey
Secondary Survey
Finalizing the topic
Research Topic Assesment and project Charter
Study the research Bacground Further
Identify the Problems more specifically
Identify the Objectives
Identify the Research Components
Create and Submit the Topic Assesment Document
Refine the Topic Assesment Document according Evaluators Feddback
Create ans Submit the Charter Document
Research Proposal
Document literature Review
Document Research Gap
Document the Objectives
Document Methodology
Document the Commercial Value
Create and Submit the proposal report
Proposal Presentation
Progress Presentation 1
Design and Implement the virtual Environment
Design and Implement the Charter Models
Enable Multiuser Access and Communication
Implement QA discussion forum
Implement Voice channel between friends
Test Core Functionalities
Progress Presentation 2
Complete Core Functionalities
Implement Collaborative Content Editing
Refine the UI and UX
Integrate Core functionalities
Test the whole component
Final Report
Document the research Outcomes
Create and submit Research
Submit Final Report
Integrate Core functionalities
Final Assesment
Integrate with other Research Components
Integration and system testing
Finalize all Deliverables
Deploy the System
Final Presentation

REFERENCES

1. “Blockchain-based Criminal Record Database Management.” [Online]. Available: https://ieeexplore.ieee.org/document/9544655. [Accessed: 19-Mar-2023].

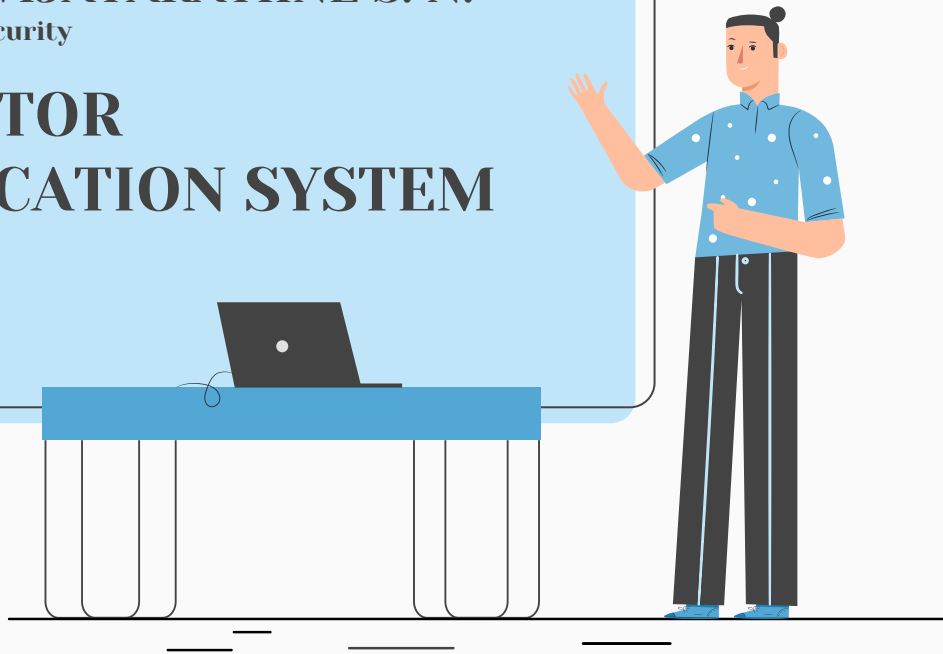
1. “Crab: Blockchain based Criminal Record Management System.” [Online]. Available: https://www.researchgate.net/publication/329489346_CRAB_Blockchain_Based_Criminal_Record_Management_System. [Accessed: 19-Mar-2023].

1. “Blockchain-based Criminal Record Database Management.” [Online]. Available: https://ieeexplore.ieee.org/document/9544655. [Accessed: 19-Mar-2023].

1. Wust, K., Gipp, B., & Breitenbücher, U. (2018). “Blockchain in forensic science: Securing digital evidence”. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1350- 1355). IEEE.

IT20171438 | WIJAYARATHNE S. N.
Specializing in Cyber Security

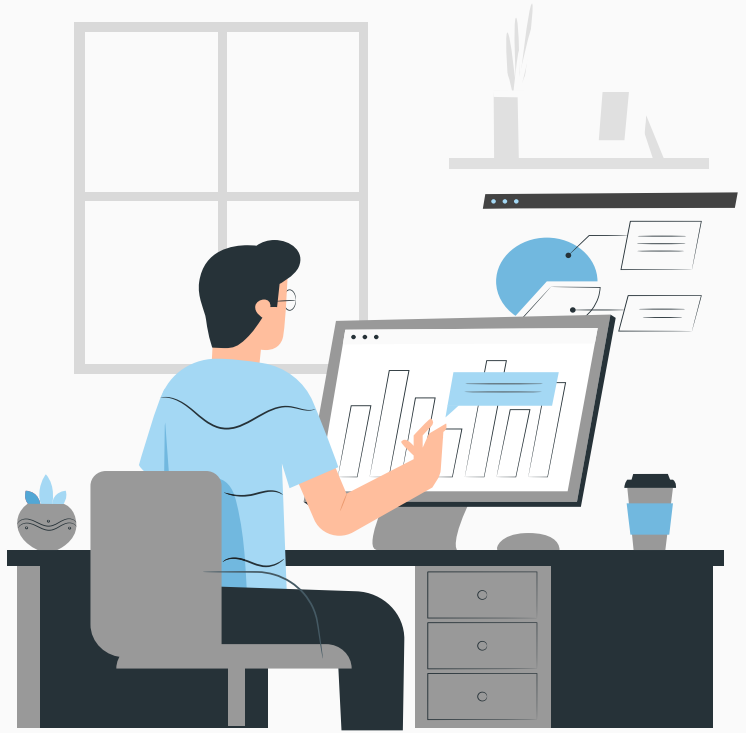
MULTIFACTOR AUTHENTICATION SYSTEM



SLIIT
FACULTY OF COMPUTING

RESEARCH QUESTION

1. RESEARCH QUESTION
2. RESEARCH GAP
3. SUB OBJECTIVES

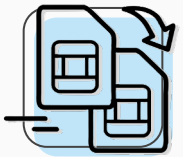


RESEARCH QUESTION

- How To Secure System Login By Implementing A Secure Authentication System To The Blockchain- Based Criminal Information Management System In Sri Lanka?

- Is 2-Factor Authentication SECURE? Can 2-Factor Authentication be HACKED?
  - SIM Swapping
  - SIM Cloning
  - Man-in-the-Middle Attacks
  - Phishing Attacks
  - Social Engineering




RESEARCH GAP

CONSIDERATION ON	EXISTING SYSTEMS	PROPOSED SYSTEM
1ST FACTOR	Security Level is **LOW**	Security Level is **HIGH**
2ND FACTOR	Security Level is **MODERATE**	Security Level is **HIGH**
3RD FACTOR	Security Level is **MODERATE**	Security Level is **HIGH**
CONFIDENTIALITY	Security Level is **LOW**	Security Level is **HIGH**
INTEGRITY	Security Level is **LOW**	Security Level is **HIGH**
POSSIBLE OTP COMBINATIONS	LOW (59,049)	HIGH (60,466,176)
ARTIFICIAL INTELLIGENCE	NONE	IMPLEMENTED
OVERALL SYSTEM	Security Level is MODERATE	Security Level is HIGH

SPECIFIC & SUB OBJECTIVES

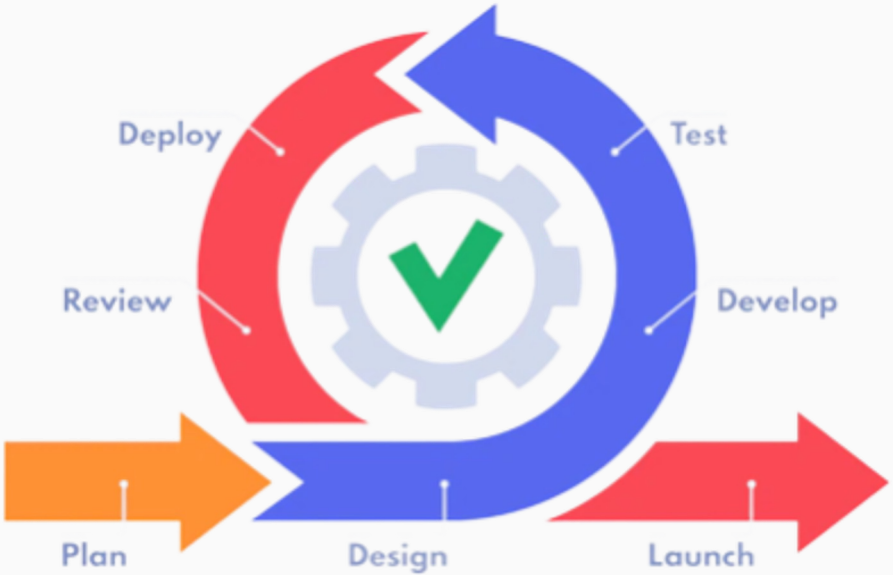
- Proposed Authentication System;
    - Three-Factor Authentication (3FA) System
    - Additional Layer of Security Implemented at the End.

- The 1st Factor;
    - Username and Password
- The 2nd Factor;
    - One-Time Password
- The 3rd Factor;
    - Facial Recognition
- Additional Layer of Security;
    - System Generated Unique Passcode

METHODOLOGY

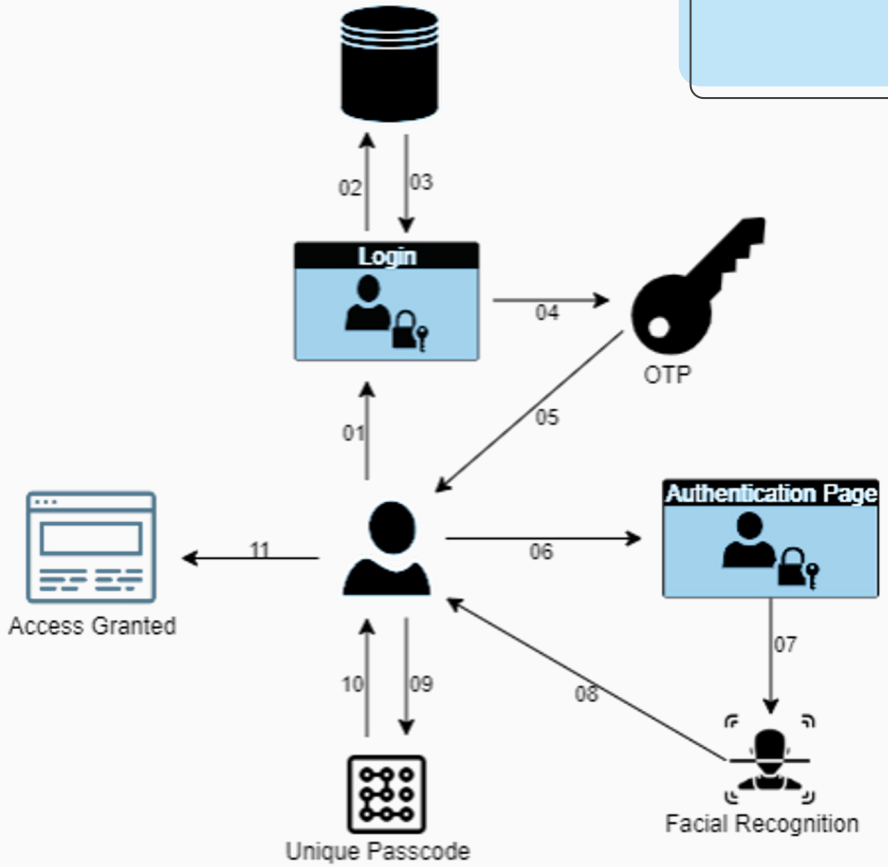
1. DEVELOPMENT CYCLE
2. SYSTEM DIAGRAM
3. SYSTEM DESCRIPTION
4. REQUIREMENTS

DEVELOPMENT CYCLE



- Why 'The Agile Life Cycle" was used?
  - Flexibility
  - Iterative Approach
  - Collaboration & Communication
  - Continuous Improvement
  - Rapid Prototyping
  - Time & Resource Management

SYSTEM DIAGRAM



01 – User entering Username & Password

02 – Entered Username & Password being checked

03 – Username & Password being verified

04 – Moving to the OTP page

05 – OTP code will be send to the client

06 – Entering the OTP code to the Authentication Page

07 – Moving to the Facial Recognition Page

08 – Facial Recognition Process

09 – User entering the Unique Passcode

10 – Verifying the Unique Passcode

11 – Access Granted to the System

SYSTEM DESCRIPTION

- 1st Factor;
  - Highest-level of Security Standards
  - Alerts Generated
  - Number of Attempts
- 2nd Factor;
  - 6-Digit Code → 6-Character Code → 60,466,176]
  - Number of Attempts
  - Time Restriction
- 3rd Factor;
  - AI Trained Algorithm
  - Number of Attempts
- Additional Layer of Security;
  - Unique System Generated Code
  - Code Expiration

[59,049

REQUIREMENTS

Functional Requirements

- User Registration
- Factor Options
- Factor Management
- Authentication Workflow
- Integration with Applications
- Authentication Logging

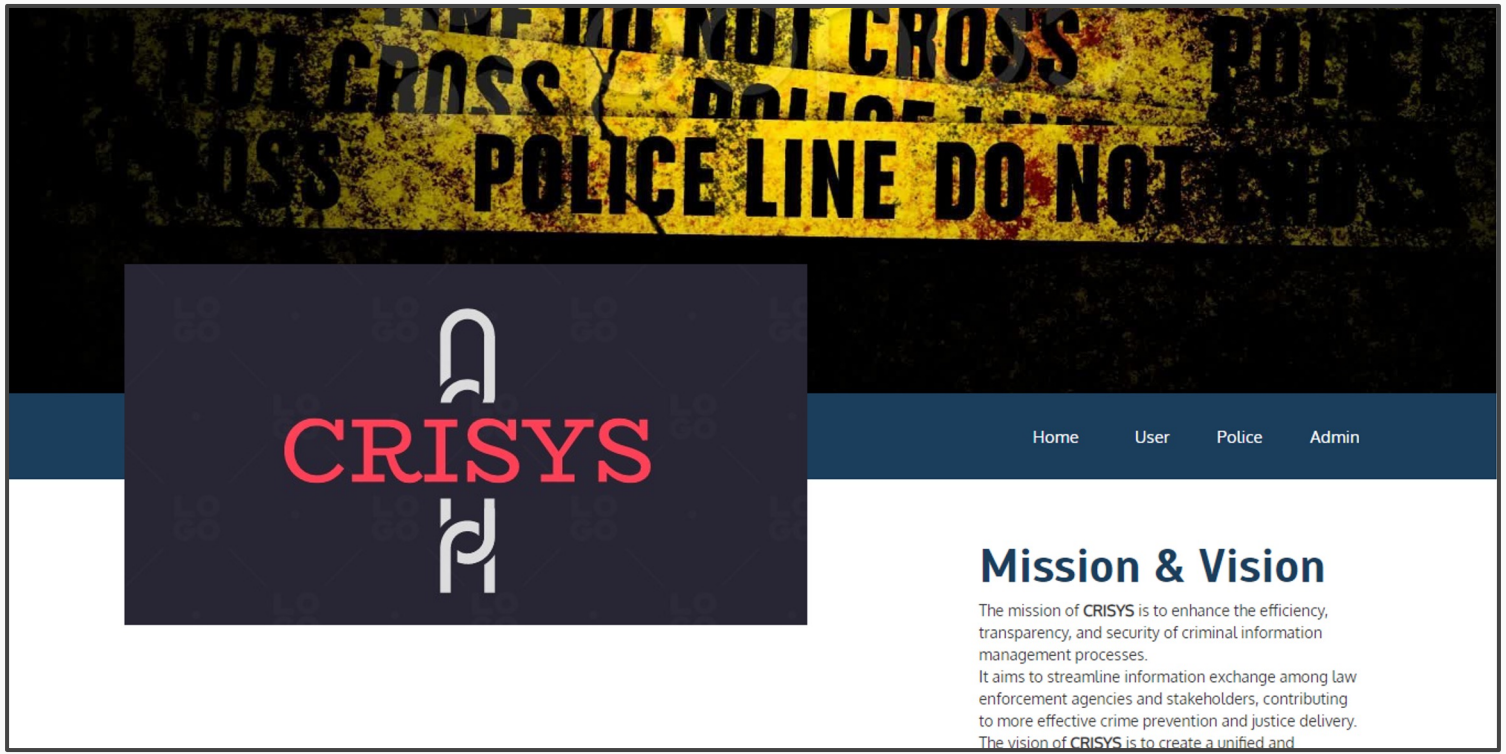
Non-Functional Requirements

- Security
- Performance
- Reliability
- Usability
- Scalability
- Compliance

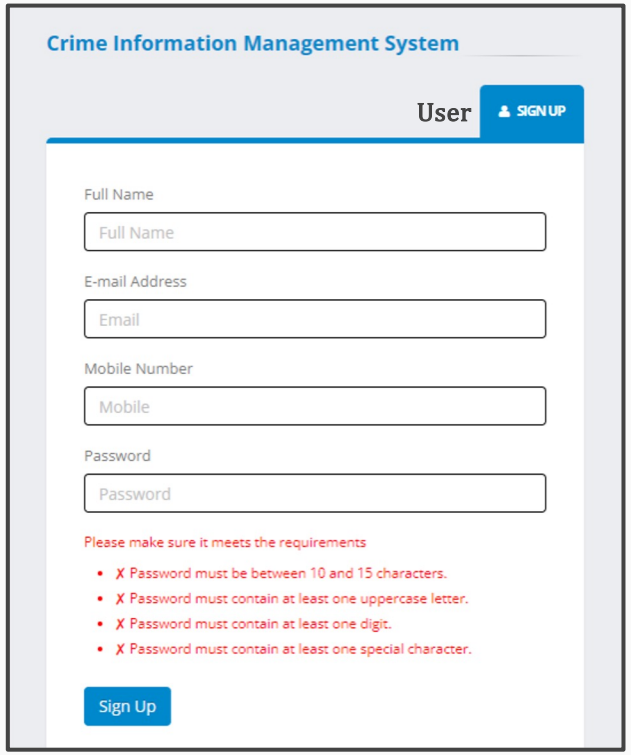
IMPLEMENTATIO N

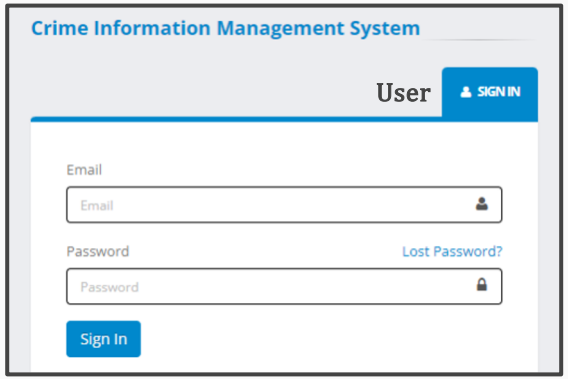
1. LAYOUTS
2. CODES
3. DATABASE
4. DATASET

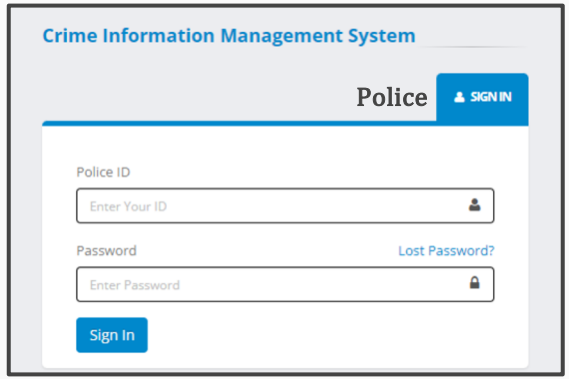
LAYOUTS

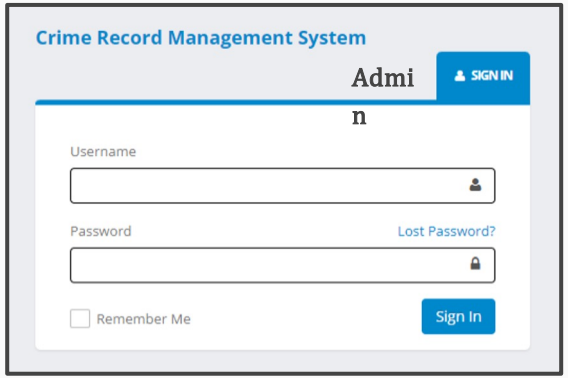

POLICE LINE DO NOT
CRISYS
Home
User
Police
Admin
Mission & Vision
The mission of CRISYS is to enhance the efficiency, transparency, and security of criminal information management processes.
It aims to streamline information exchange among law enforcement agencies and stakeholders, contributing to more effective crime prevention and justice delivery.
The vision of CRISYS is to create a unified and

LAYOUTS


Crime Information Management System
User
SIGN UP
Full Name
Full Name
E-mail Address
Email
Mobile Number
Mobile
Password
Password
Please make sure it meets the requirements
✗ Password must be between 10 and 15 characters.
✗ Password must contain at least one uppercase letter.
✗ Password must contain at least one digit.
✗ Password must contain at least one special character.
Sign Up


Crime Information Management System
User
SIGN IN
Email
Email
Password
Lost Password?
Password
Sign In

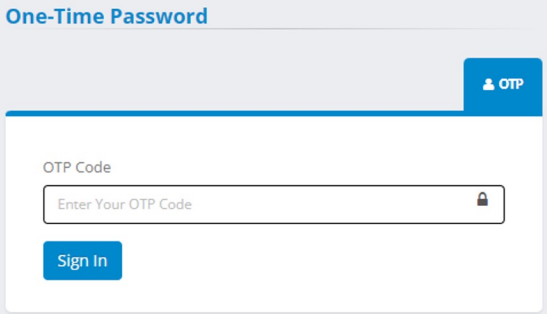

Crime Information Management System
Police
SIGN IN
Police ID
Enter Your ID
Password
Lost Password?
Enter Password
Sign In


Crime Record Management System
Admin
SIGN IN
Username
Password
Lost Password?
Remember Me
Sign In

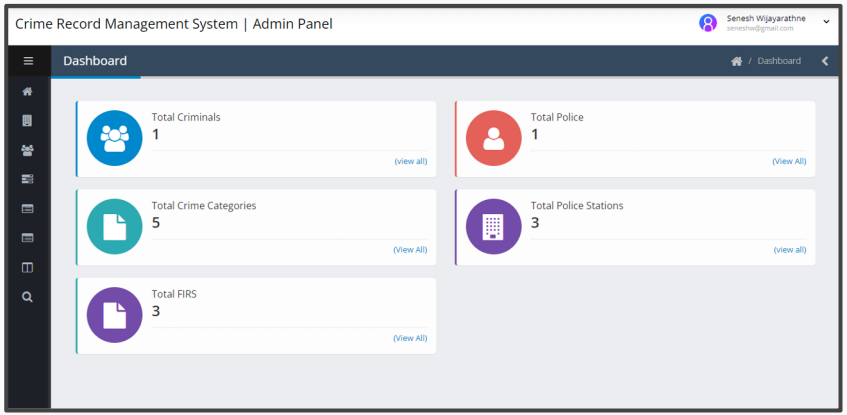
LAYOUTS

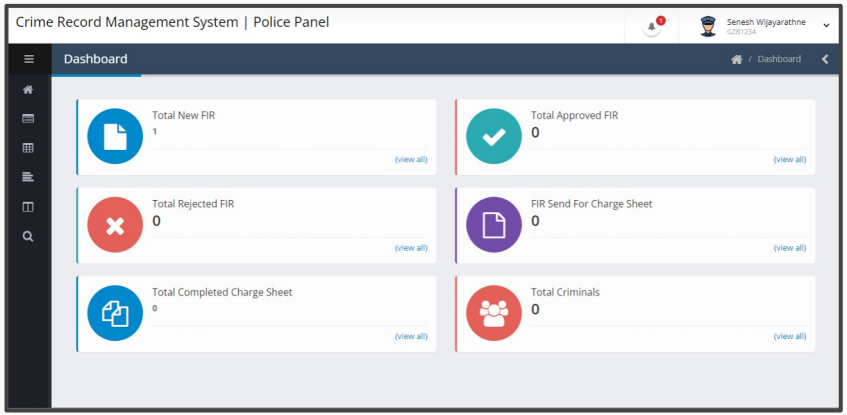
One-Time Password: KK7c0p

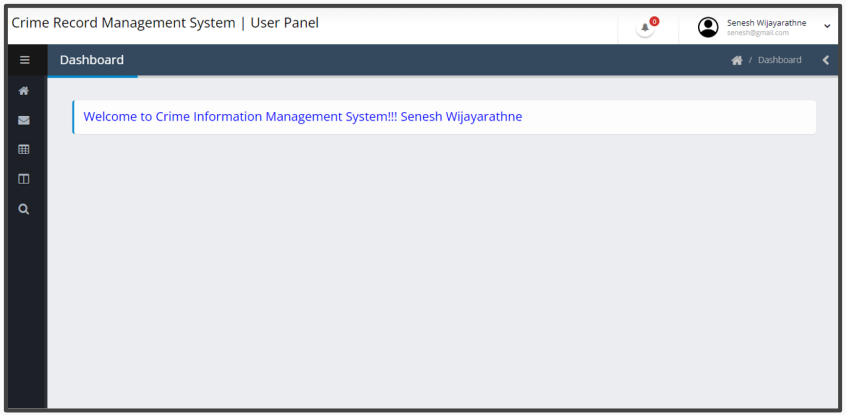
Time remaining: 44 seconds



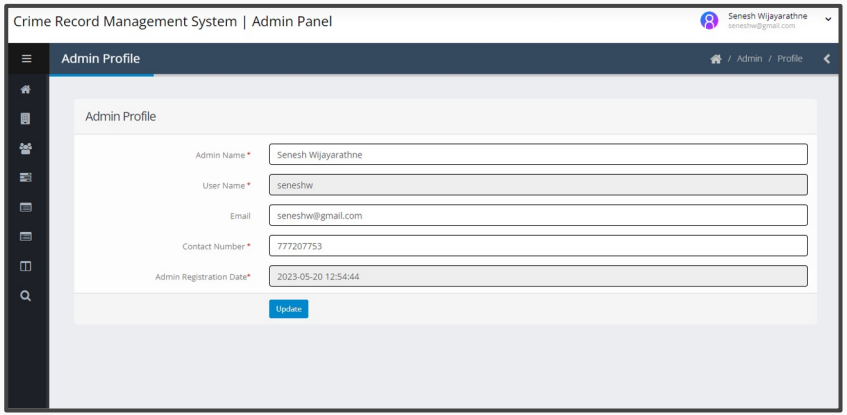
LAYOUTS

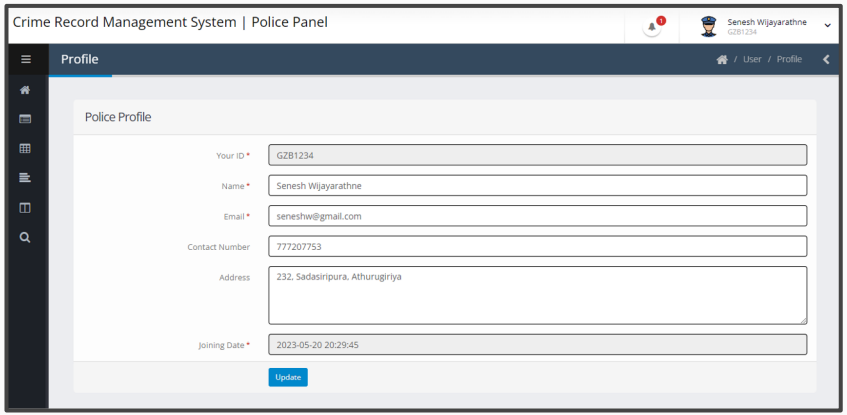

Crime Record Management System | Admin Panel
Senesh Wijayarathne
Dashboard
Dashboard
Total Criminals
1
(view all)
Total Police
1
(View All)
Total Crime Categories
5
(View All)
Total Police Stations
3
(view all)
Total FIRS
3
(View All)

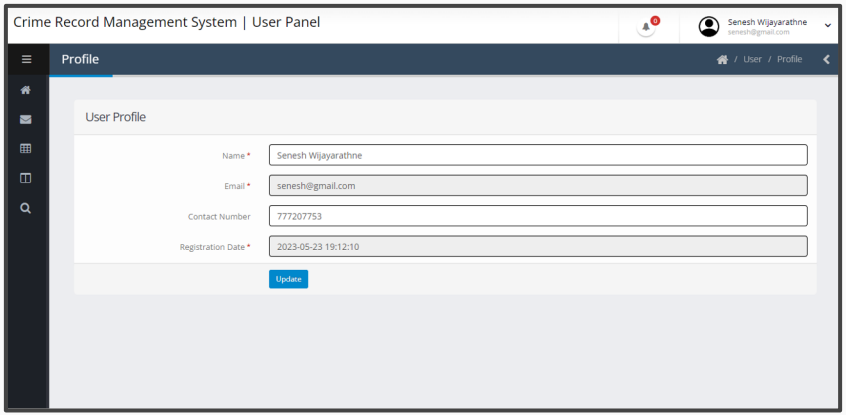

Crime Record Management System | Police Panel
Senesh Wijayarathne
Dashboard
Dashboard
Total New FIR
1
(view all)
Total Approved FIR
0
(view all)
Total Rejected FIR
0
(view all)
FIR Send For Charge Sheet
0
(view all)
Total Completed Charge Sheet
0
(view all)
Total Criminals
0
(view all)


Crime Record Management System | User Panel
Senesh Wijayarathne
Dashboard
Dashboard
Welcome to Crime Information Management System!!! Senesh Wijayarathne

LAYOUTS


Crime Record Management System | Admin Panel
Senesh Wijayarathne
seneshw@gmail.com
Admin Profile
Admin / Profile
Admin Profile
Admin Name *
Senesh Wijayarathne
User Name *
seneshw
Email
seneshw@gmail.com
Contact Number *
777207753
Admin Registration Date*
2023-05-20 12:54:44
Update


Crime Record Management System | Police Panel
Senesh Wijayarathne
GZB1234
Profile
User / Profile
Police Profile
Your ID *
GZB1234
Name *
Senesh Wijayarathne
Email *
seneshw@gmail.com
Contact Number
777207753
Address
232, Sadasiripura, Athurugiriya
Joining Date *
2023-05-20 20:29:45
Update


Crime Record Management System | User Panel
Senesh Wijayarathne
senesh@gmail.com
Profile
User / Profile
User Profile
Name *
Senesh Wijayarathne
Email *
senesh@gmail.com
Contact Number
777207753
Registration Date *
2023-05-23 19:12:10
Update

CODE

signup.php

```
<script>
    $(document).ready(function() {
        $('#password').on('input', function() {
            var password = $(this).val();
            var regex = /^(?=.*[A-Z])(?=.*\d)(?=.*[!@#$%^&*()\-_=+{};:,<.>]).{10,15}$/;

            var hasUpperCase = /[A-Z]/.test(password);
            var hasDigit = /\d/.test(password);
            var hasSpecialChar = /[!@#$%^&*()\-_=+{};:,<.>]/.test(password);
            var isLengthValid = (password.length >= 10 && password.length <= 15);

            var criteriaList = $('#passwordCriteria');
            criteriaList.empty();

            if (!isLengthValid) {
                criteriaList.append('<li>✘ Password must be between 10 and 15 characters.</li>');
            } else {
                criteriaList.append('<li class="valid">✔ Password must be between 10 and 15 characters.</li>');
            }

            if (!hasUpperCase) {
                criteriaList.append('<li>✘ Password must contain at least one uppercase letter.</li>');
            } else {
                criteriaList.append('<li class="valid">✔ Password must contain at least one uppercase letter.</li>');
            }

            if (!hasDigit) {
                criteriaList.append('<li>✘ Password must contain at least one digit.</li>');
            } else {
                criteriaList.append('<li class="valid">✔ Password must contain at least one digit.</li>');
            }

            if (!hasSpecialChar) {
                criteriaList.append('<li>✘ Password must contain at least one special character.</li>');
            } else {
                criteriaList.append('<li class="valid">✔ Password must contain at least one special character.</li>');
            }

            if (!regex.test(password)) {
                $('#passwordFeedback').text('Please make sure it meets the requirements');
            } else {
                $('#passwordFeedback').text('');
            }
        });
    });
</script>
```

signin1.php

```
<?php
session_start();
error_reporting(0);
include('includes/dbconnection.php');
$maxAttempts = 5; // Maximum number of login attempts
$lockoutTime = 300; // Lockout time in seconds (5 minutes)
$extendedLockoutTime = 3600; // Extended lockout time in seconds (1 hour)
if (isset($_SESSION['login_attempts']) && $_SESSION['login_attempts'] >= $maxAttempts) {
    // User is locked out, check lockout time
    $lockoutEndTime = $_SESSION['lockout_time'] + $lockoutTime;
    if (time() < $lockoutEndTime) {
        $remainingTime = $lockoutEndTime - time();
        echo "<script>alert('You are locked out. Please try again after $remainingTime seconds.');</script>";
        exit();
    } else {
        // Lockout time has expired, reset login attempts
        unset($_SESSION['login_attempts']);
        unset($_SESSION['lockout_time']);
    }
}
if (isset($_POST['login'])) {
    $pid = $_POST['pid'];
    $password = md5($_POST['password']);
    $sql = "SELECT ID, PID, PoliceStationId FROM tblpolice WHERE PID = :pid AND Password = :password";
    $query = $dbh->prepare($sql);
    $query->bindParam(':pid', $pid, PDO::PARAM_STR);
    $query->bindParam(':password', $password, PDO::PARAM_STR);
    $query->execute();
    $results = $query->fetchAll(PDO::FETCH_OBJ);
    if ($query->rowCount() > 0) {
        foreach ($results as $result) {
            $_SESSION['crmspid'] = $result->ID;
            $_SESSION['crmsipid'] = $result->PID;
            $_SESSION['psid'] = $result->PoliceStationId;
        }
        $_SESSION['login'] = $_POST['pid'];
        unset($_SESSION['login_attempts']); // Reset login attempts
        echo "<script type='text/javascript'> document.location ='otp02.php'; </script>";
    } else {
        if (!isset($_SESSION['login_attempts'])) {
            $_SESSION['login_attempts'] = 1;
        } else {
            $_SESSION['login_attempts']++;
        }
        if ($_SESSION['login_attempts'] >= $maxAttempts) {
            // Reached maximum login attempts
            $_SESSION['lockout_time'] = time(); // Set lockout time
            echo "<script>alert('Invalid Details. You are locked out for $lockoutTime seconds.');</script>";
            exit();
        } else {
            echo "<script>alert('Invalid Details');</script>";
        }
    }
}
?>
```

CODE

send-email.php

```php
<?php
use PHP<ailer\PHPMailer\PHPMailer;

require_once 'PHPMailer/src/Exception.php';
require_once 'PHPMailer/src/PHPMailer.php';
require_once 'PHPMailer/src/SMTP.php';

$mail = new PHPMailer(true);

if(isset($_POST['submit'])){
    $OPTcode = $_POST['name'];

    try{
        $mail->isSMTP();
        $mail->Host = 'smtp.gmail.com';
        $mail->SMTPAuth = true;
        $mail->Username = 'yourmail@gmail.com'; //Need to enter Username
        $mail->Password = '[Password]'; //Need to enter the Password
        $mail->SMTPSecure = "tls";
        $mail->Port = '587';

        $mail->setFrom('yourmail@gmail.com'); //Need to enter Username
        $mail->addAddress('Gmail Address'); //Need to read the file from the DB and config data

        $mail->isHTML(true)
        $mail->Subject = 'Your One-Time Password is:'. $OTPcode;
        $mail->Body = "Please enter the follwoing as your One-Time Password to login to the system. <br>One-Time Password: $OTPCode";

    }
}
```

otp02.php

```php
<?php
session_start();
error_reporting(0);
include('includes/dbconnection.php');
// Function to generate a random 6-character password
function generatePassword() {
    $characters = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
    $password = '';
    for ($i = 0; $i < 6; $i++) {
        $index = rand(0, strlen($characters) - 1);
        $password .= $characters[$index];
    }
    return $password;
}
// Set or retrieve the password from the session
if (isset($_SESSION['password'])) {
    $password = $_SESSION['password'];
} else {
    $password = generatePassword();
    $_SESSION['password'] = $password;
}
// Set or retrieve the expiration time from the session
if (isset($_SESSION['expiration'])) {
    $expiration = $_SESSION['expiration'];
} else {
    $expiration = time() + 60;
    $_SESSION['expiration'] = $expiration;
}
// Update the password and expiration time every 60 seconds
if (time() > $expiration) {
    $password = generatePassword();
    $_SESSION['password'] = $password;
    $expiration = time() + 60;
    $_SESSION['expiration'] = $expiration;
}
// Display the password and countdown timer
echo "<h2>One-Time Password: $password</h2>";
$remainingTime = $expiration - time();
echo "<h3>Time remaining: <span id='countdown'>$remainingTime</span> seconds</h3>";

// Verify the entered password
if (isset($_POST['otp'])) {
    $enteredPassword = $_POST['otp'];
    if ($enteredPassword === $password) {
        echo "<script type='text/javascript'> document.location ='dashboard.php'; </script>";
    } else {
        echo "<p>Incorrect password. Please try again.</p>";
    }
}
?>
```

DATABASE

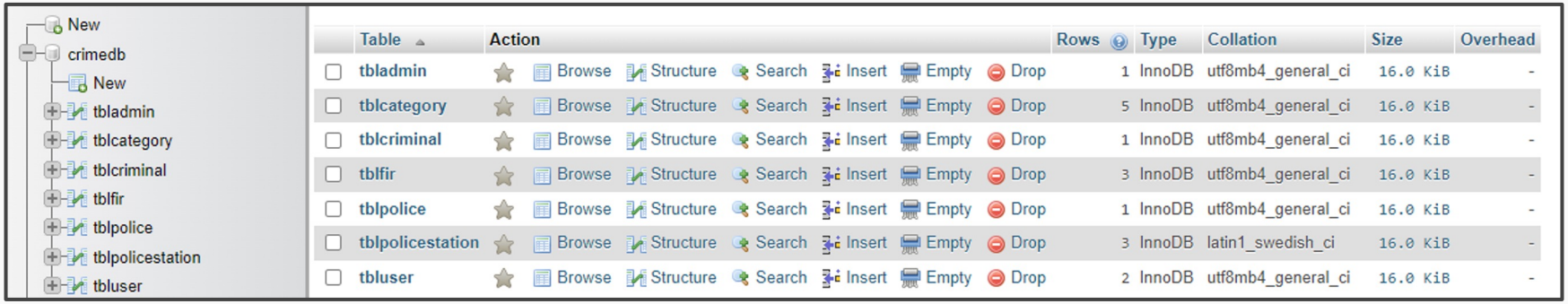


Table	Action	Rows	Type	Collation	Size	Overhead
tbladmin	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_general_ci	16.0 KiB	-
tblcategory	Browse Structure Search Insert Empty Drop	5	InnoDB	utf8mb4_general_ci	16.0 KiB	-
tblcriminal	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_general_ci	16.0 KiB	-
tblfir	Browse Structure Search Insert Empty Drop	3	InnoDB	utf8mb4_general_ci	16.0 KiB	-
tblpolice	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_general_ci	16.0 KiB	-
tblpolicestation	Browse Structure Search Insert Empty Drop	3	InnoDB	latin1_swedish_ci	16.0 KiB	-
tbluser	Browse Structure Search Insert Empty Drop	2	InnoDB	utf8mb4_general_ci	16.0 KiB	-

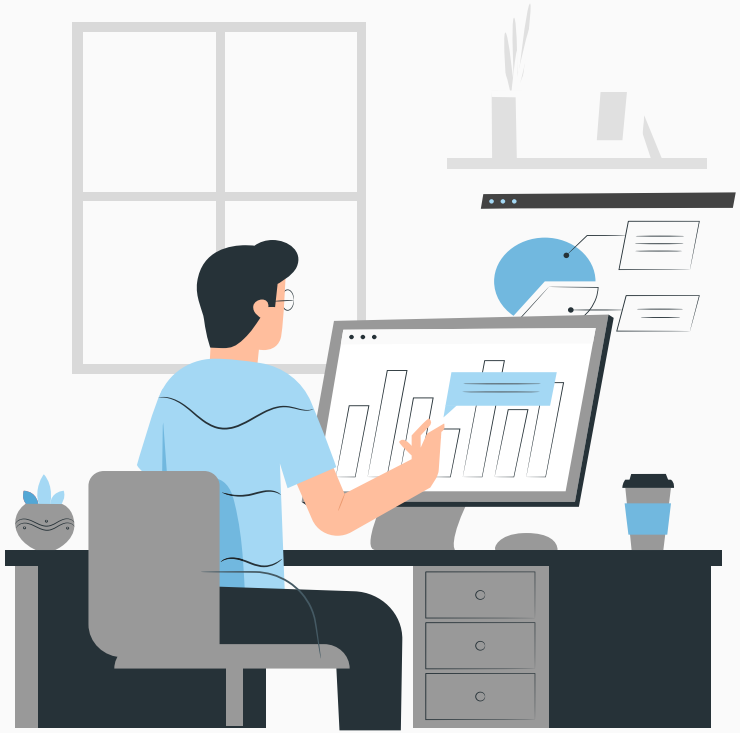
DATASET

DEMONSTRATION

1. USER SIGN UP & SIGN IN
2. ADMIN & POLICE OFFICER SIGN IN
3. ACCOUNT LOCK
4. 6-CHARACTER CODE & VALIDATION
5. ALL USER PROFILES
6. ~~DASHBOARDS~~

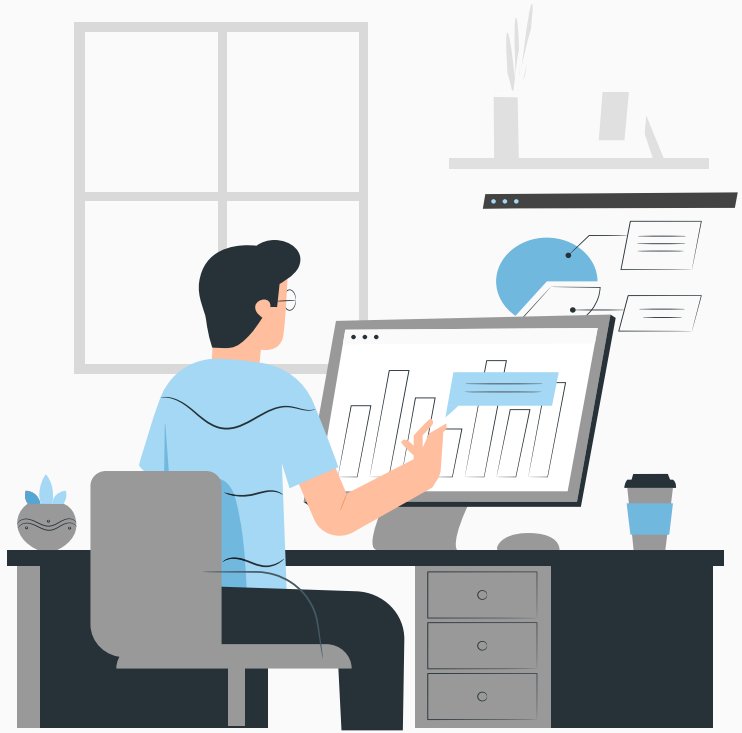
PENDING WORK

1. SETUP SMTP & SMS GATEWAY PROVIDER
2. IMPLEMENT FACIAL RECOGNITION
3. INTEGRATE WITH OTHER SYSTEM

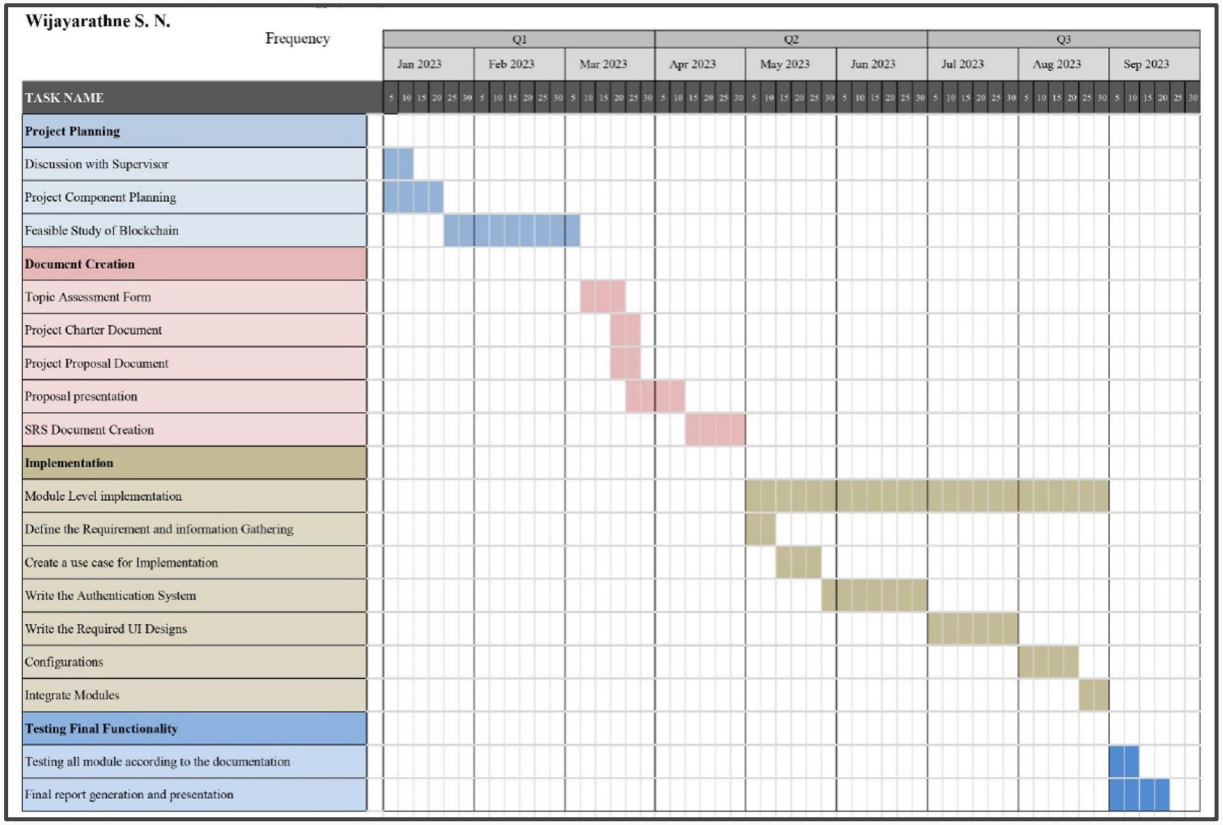


OTHER INFORMATION

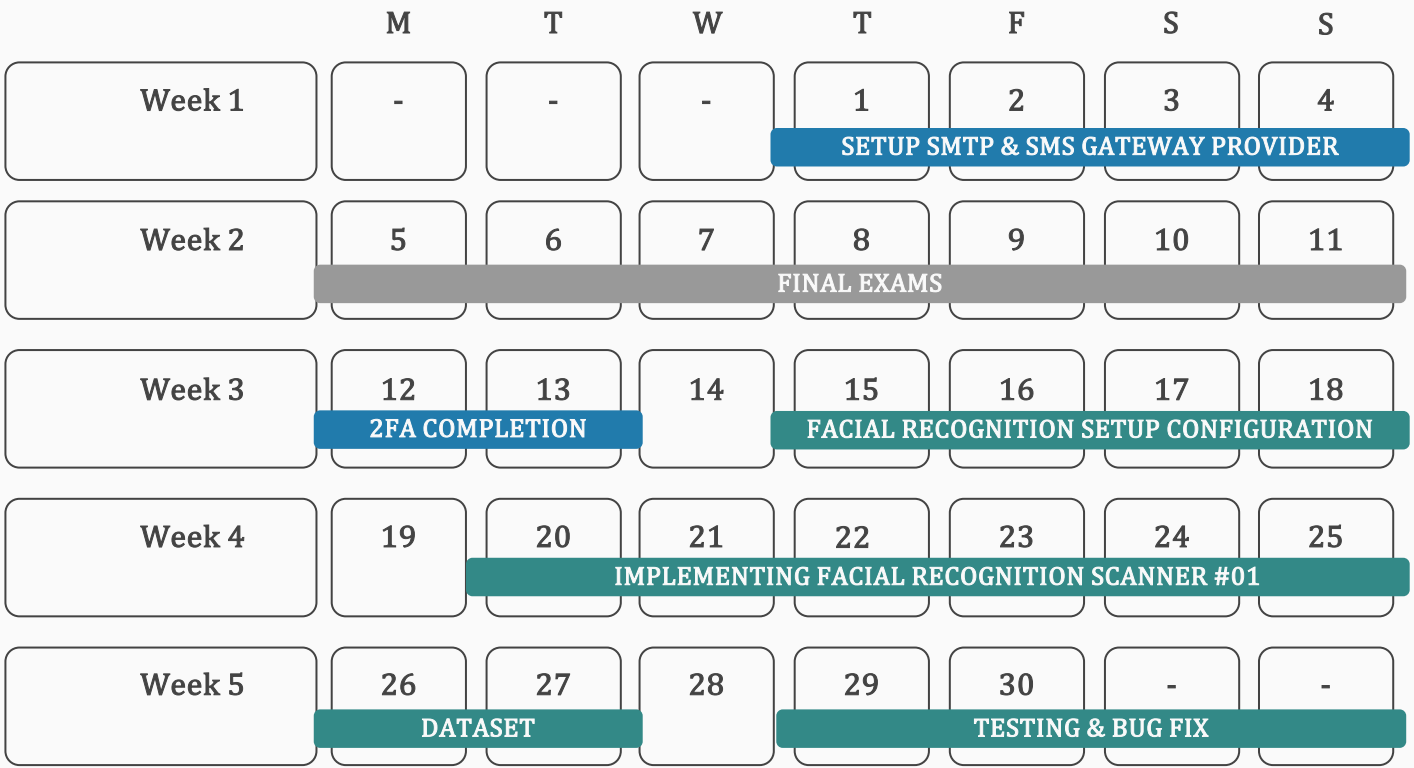
1. GANTT CHART
2. SCHEDULE
3. REFERENCES



GANTT CHART


Wijayarathne S. N.
Frequency
Q1
Q2
Q3
Jan 2023
Feb 2023
Mar 2023
Apr 2023
May 2023
Jun 2023
Jul 2023
Aug 2023
Sep 2023
TASK NAME
Project Planning
Discussion with Supervisor
Project Component Planning
Feasible Study of Blockchain
Document Creation
Topic Assessment Form
Project Charter Document
Project Proposal Document
Proposal presentation
SRS Document Creation
Implementation
Module Level implementation
Define the Requirement and information Gathering
Create a use case for Implementation
Write the Authentication System
Write the Required UI Designs
Configurations
Integrate Modules
Testing Final Functionality
Testing all module according to the documentation
Final report generation and presentation

SCHEDULE


M
T
W
T
F
S
S
Week 1
-
-
-
1
2
3
4
SETUP SMTP & SMS GATEWAY PROVIDER
Week 2
5
6
7
8
9
10
11
FINAL EXAMS
Week 3
12
13
14
15
16
17
18
2FA COMPLETION
FACIAL RECOGNITION SETUP CONFIGURATION
Week 4
19
20
21
22
23
24
25
IMPLEMENTING FACIAL RECOGNITION SCANNER #01
Week 5
26
27
28
29
30
-
-
DATASET
TESTING & BUG FIX

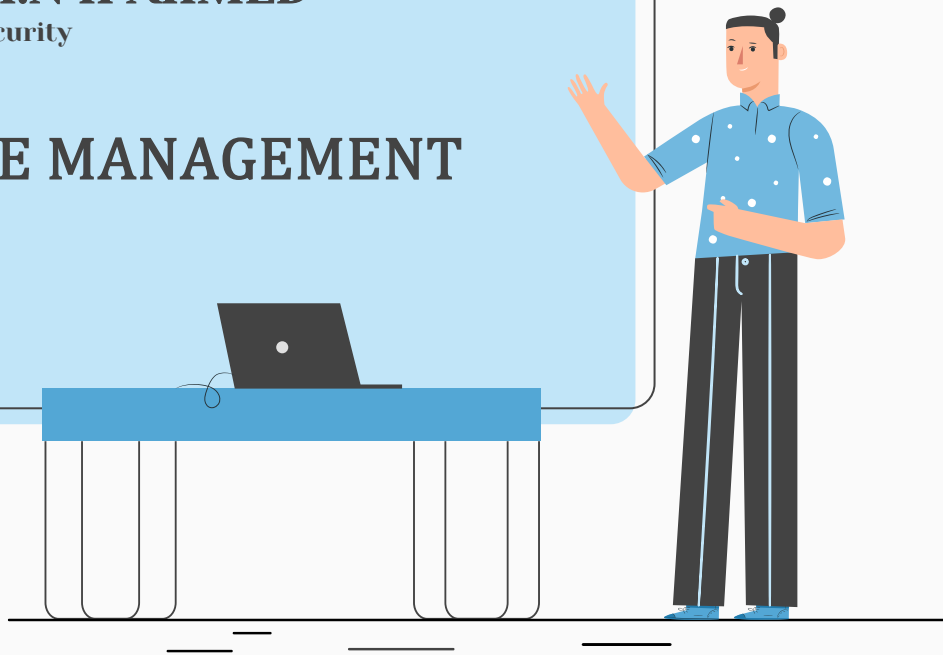
REFERENCES

- R. P. Jover, "Security analysis of SMS as a second factor of authentication," Commun. ACM, vol. 63, no. 12, p. 46–52, 17 November 2020, doi: doi.org/10.1145/3424260
- V. Papaspirou, L. Maglaras, M. A. Ferrag, I. Kantzavelou, H. Janicke and C. Douligeris, "A novel Two-Factor HoneyToken Authentication Mechanism," 2021 International Conference on Computer Communications and Networks (ICCCN), Athens, Greece, 2021, pp. 1-7, doi: 10.1109/ICCCN52240.2021.9522319.
- Konoth, R.K., van der Veen, V., Bos, H. (2017). How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication. In: Grossklags, J., Preneel, B. (eds) Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science, vol 9603. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-54970-4_24
- Adham, M., Azodi, A., Desmedt, Y., Karaolis, I. (2013). How to Attack Two-Factor Authentication Internet Banking. In: Sadeghi, AR. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39884-1_27

IT20157814 | M.N H AHMED

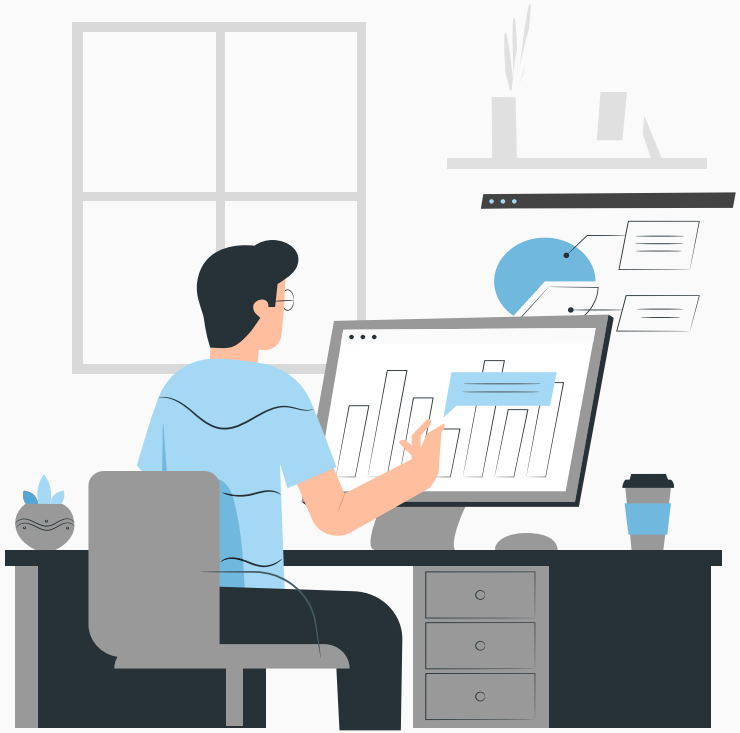
Specializing in Cyber Security

SECURE FILE MANAGEMENT SYSTEM



RESEARCH QUESTION

1. RESEARCH QUESTION
2. RESEARCH GAP
3. SUB OBJECTIVES



RESEARCH QUESTION

- How can Implementing secure file management system to ensure confidentiality, integrity, and availability of the files, in blockchain based criminal information management system for Sri Lanka?

RESEARCH GAP

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

SPECIFIC & SUB OBJECTIVES

- Implementing cryptography secure file management system to share file
- Implementing cryptography secure file management system to store file.
- Ensure Confidentiality, Integrity, Availability.
- Increase the performance and usability of criminal Records.

METHODOLOGY

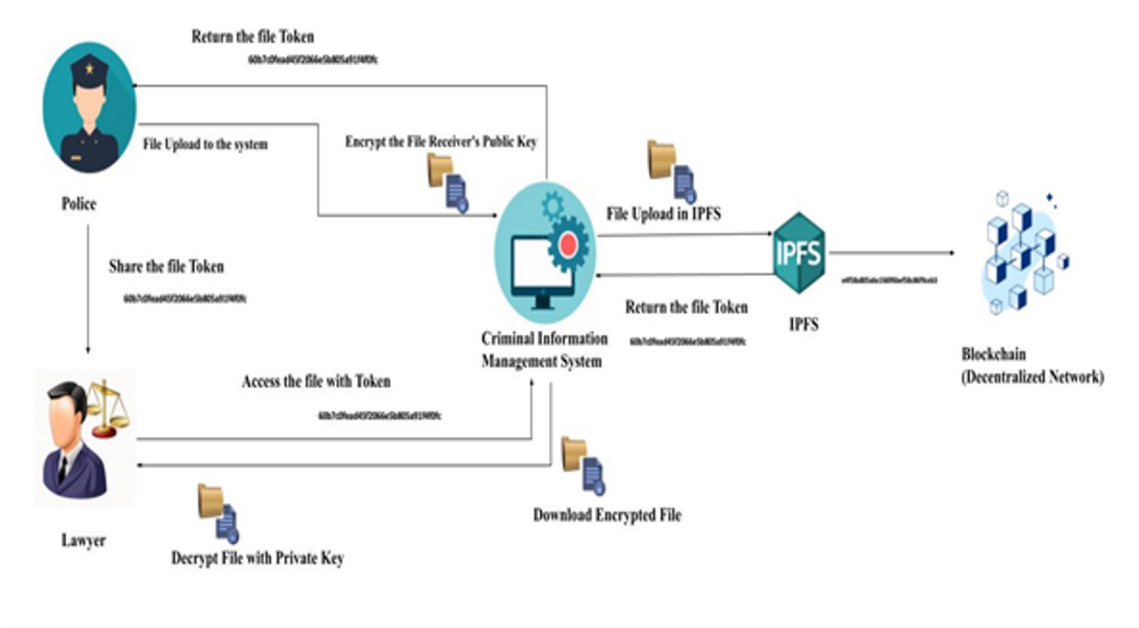
1. DEVELOPMENT CYCLE
2. SYSTEM DIAGRAM
3. SYSTEM DESCRIPTION
4. REQUIREMENTS

DEVELOPMENT CYCLE

- 'The Agile Life Cycle" was used

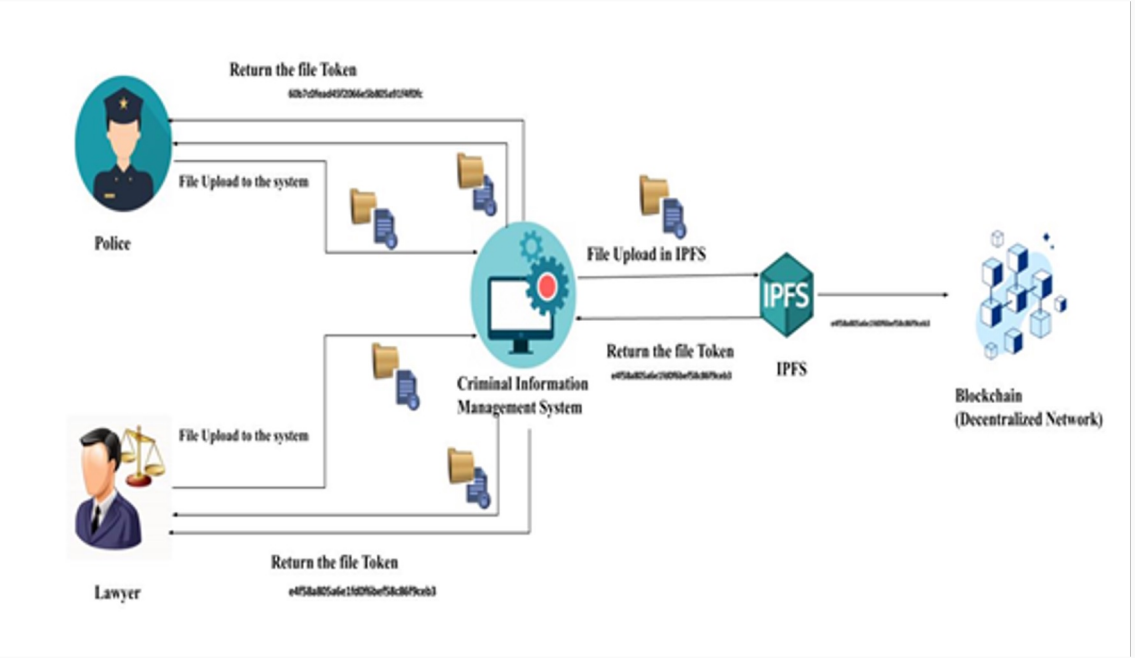
SYSTEM DIAGRAM

1.Implementing cryptography secure file management system to share file



SYSTEM DIAGRAM

2. Implementing cryptography secure file management system to store file



REQUIREMENTS

Functional Requirements

- Criminal Evidence Upload
  - FIR, Document, Image, Video and etc.
- Data Privacy and Security
- Integration with Criminal System and Blockchain

Non-Functional Requirements

- Security
- Performance
- Reliability
- Usability
- Scalability

IMPLEMENTATION

- Cryptography To Encrypt and Decrypt File
- IPFS

FILE ENCRYPTION AND DECRYPTION

File Encryption/Decryption

Choose File | No file chosen | Encryption Key: | Encrypt File

Decryption Key: | Decrypt File

Are you lost? WE GOT YOU!

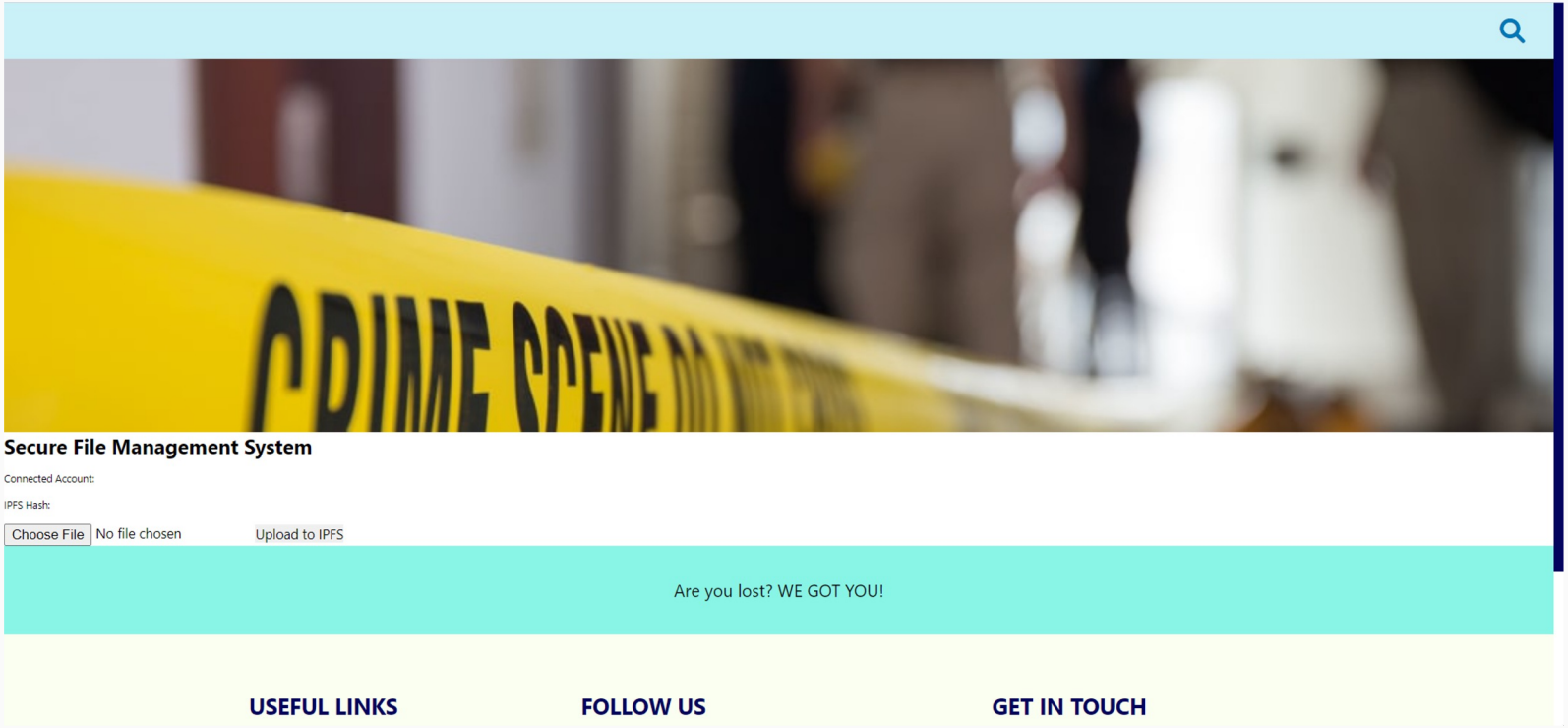
USEFUL LINKS **FOLLOW US** **GET IN TOUCH**

CODE

encrypt_and_decrypt.html > html > body > script > decryptFile

```
66
67      <h1>File Encryption/Decryption</h1><br>
68
69      <input type="file" id="fileInput">
70      <label for="encryptionKey">Encryption Key:</label>
71      <input type="text" id="encryptionKey">
72      <button onclick="encryptFile()">Encrypt File</button>
73      <br>
74      <br>
75      <label for="decryptionKey">Decryption Key:</label>
76      <input type="text" id="decryptionKey">
77      <button onclick="decryptFile()">Decrypt File</button>
78
79      <script src="https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.0.0/crypto-js.min.js"></script>
80      <script>
81        function encryptFile() {
82          const fileInput = document.getElementById('fileInput');
83          const file = fileInput.files[0];
84          const encryptionKey = document.getElementById('encryptionKey').value;
85
86          if (file && encryptionKey) {
87            const reader = new FileReader();
88            reader.onload = function(e) {
89              const encryptedData = encrypt(e.target.result, encryptionKey);
90              downloadFile(encryptedData, file.name + '.enc');
91            };
92            reader.readAsArrayBuffer(file);
93          } else {
94            alert('Please select a file and enter an encryption key.');
95          }
96        }
97
98        function decryptFile() {
99          const fileInput = document.getElementById('fileInput');
100         const file = fileInput.files[0];
101         const decryptionKey = document.getElementById('decryptionKey').value;
102
```

FILE UPLOAD TO IPFS

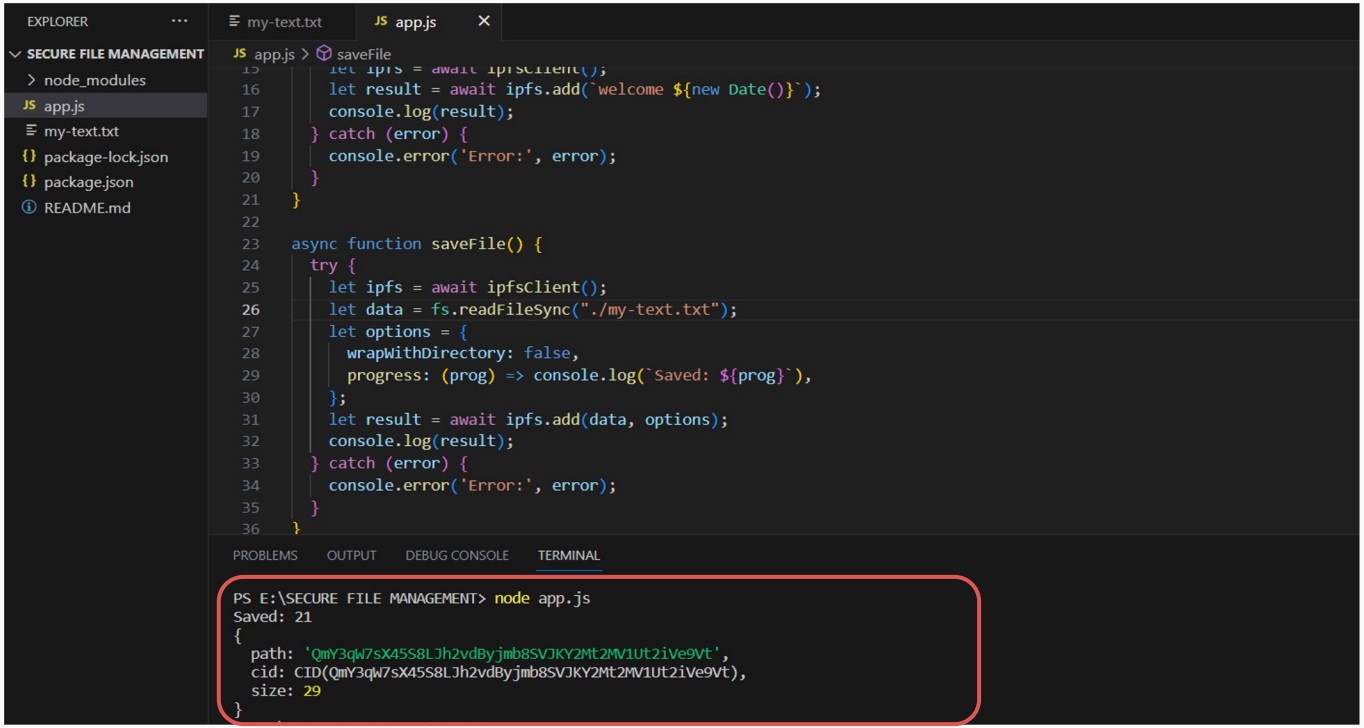


CODE

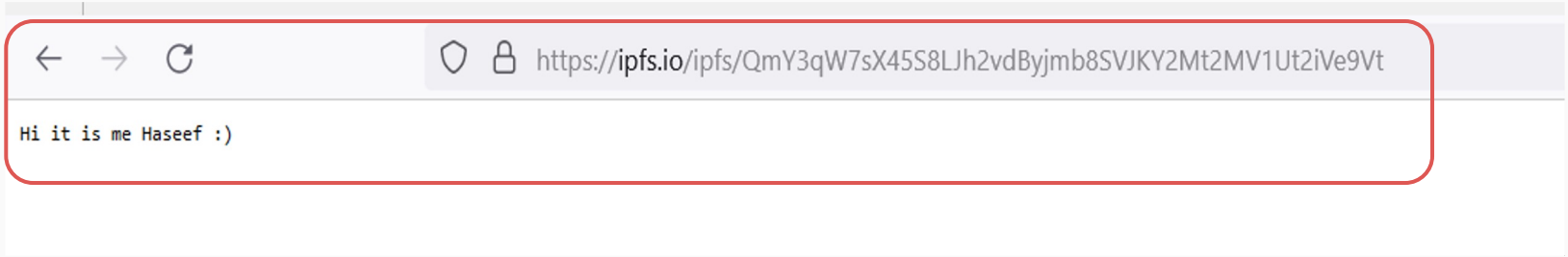
upload_file.html > html > body > div.heading2

```
<h1>Secure File Management System</h1> <br>

<p>Connected Account: <span id="account"></span></p><br>

<p>IPFS Hash: <span id="ipfsHash"></span></p><br>

<form>
  <input type="file" id="fileInput">
  <button onclick="uploadToIPFS()">Upload to IPFS</button>
</form>

<script>
  // Check if Web3 is available
  if (typeof web3 !== 'undefined') {
    // Use existing provider (e.g., MetaMask)
    web3 = new Web3(web3.currentProvider);
  } else {
    // Set up a new provider (e.g., localhost)
    web3 = new Web3(new Web3.providers.HttpProvider('http://localhost:8545'));
  }

  // Set the default account
  web3.eth.defaultAccount = web3.eth.accounts[0];

  // Set the contract address and ABI
  const contractAddress = '0x123456789abcdef...';
  const contractABI = [
    // Add your contract's ABI here
  ];

  // Create an instance of the contract
  const contract = new web3.eth.Contract(contractABI, contractAddress);

  // Get the connected account
  const getAccount = async () => {
    const accounts = await web3.eth.getAccounts();
    const account = accounts[0];
```

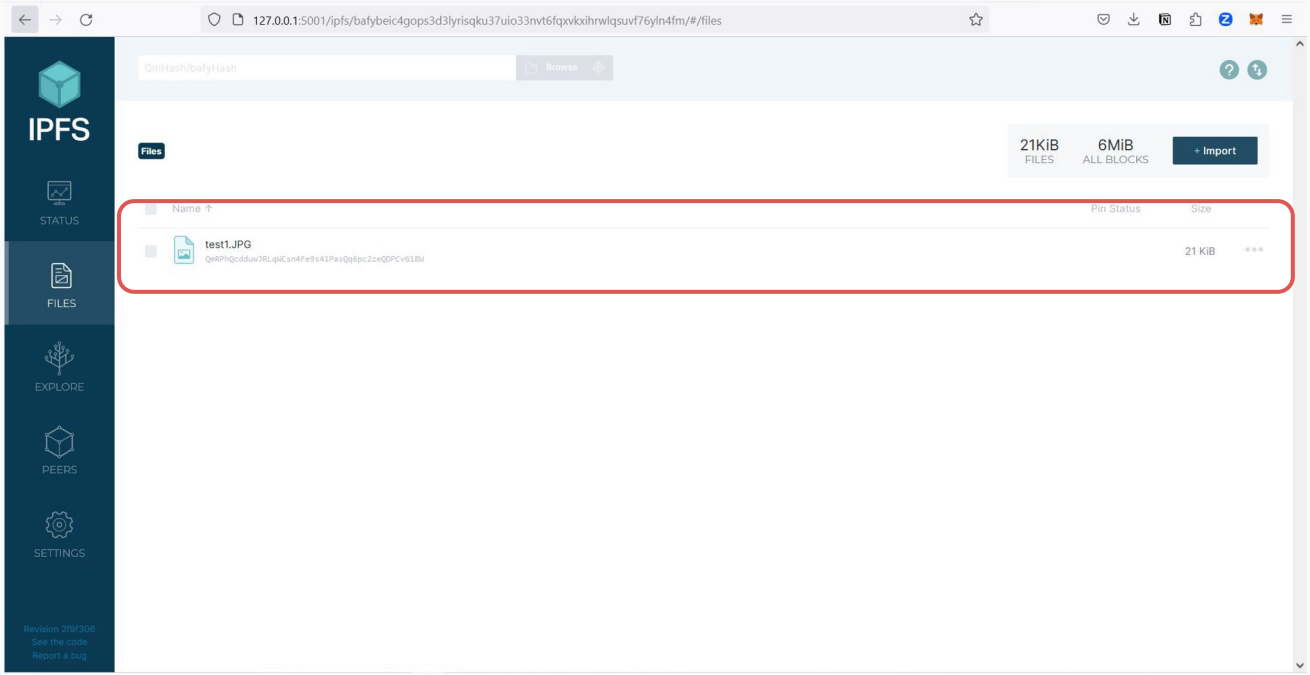
FILE UPLOAD TO IPFS AND RETRIEVE “CID” VALUE OF THE FILE



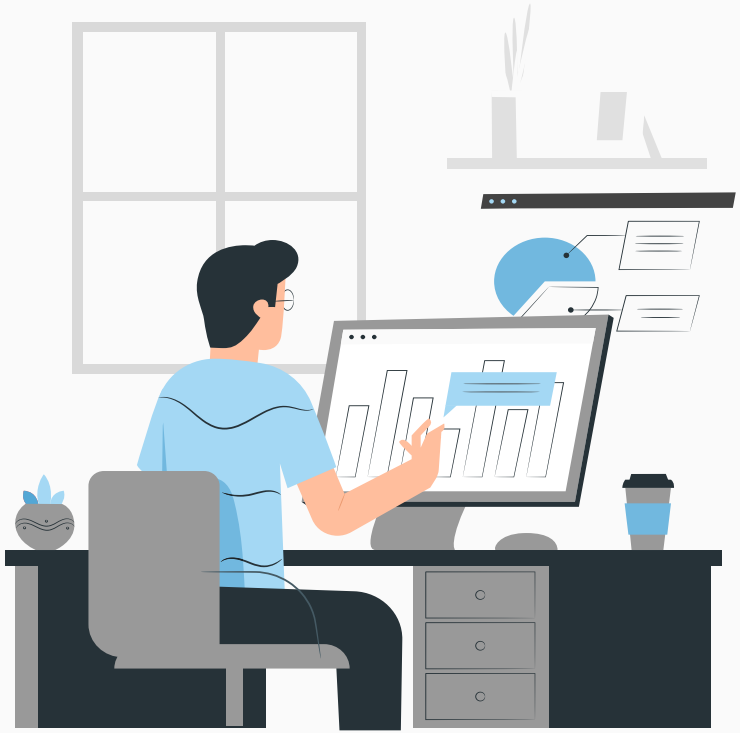
FILE UPLOAD TO IPFS



IPFS SYSTEM

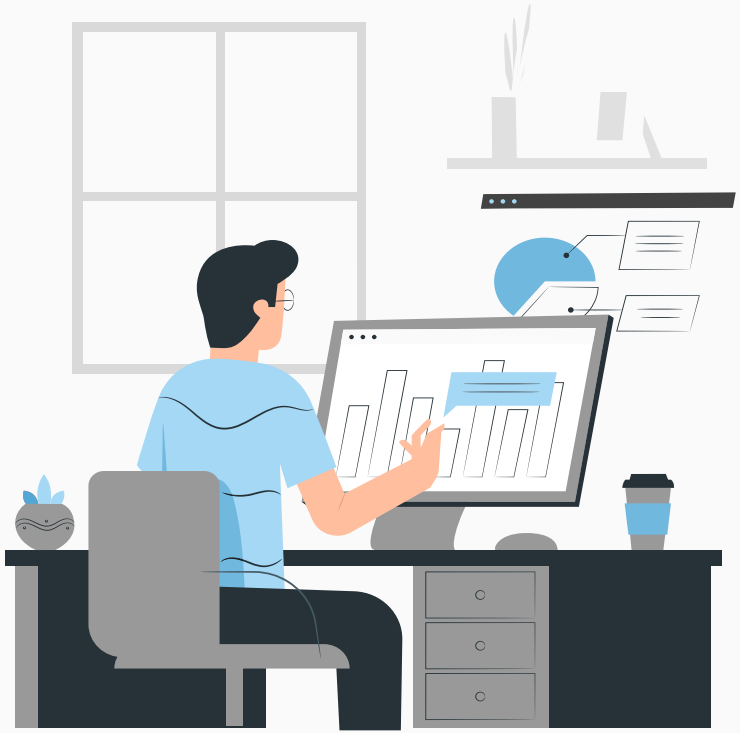

127.0.0.1:5001/ipfs/bafybeic4gops3d3lyrisqku37uio33nvt6fqxvkxihrwlqsuvf76yln4fm/#/files
IPFS
STATUS
FILES
EXPLORE
PEERS
SETTINGS
Files
21KiB
FILES
6MiB
ALL BLOCKS
+ Import
Name
Pin Status
Size
test1.JPG
21 KiB

Demonstration



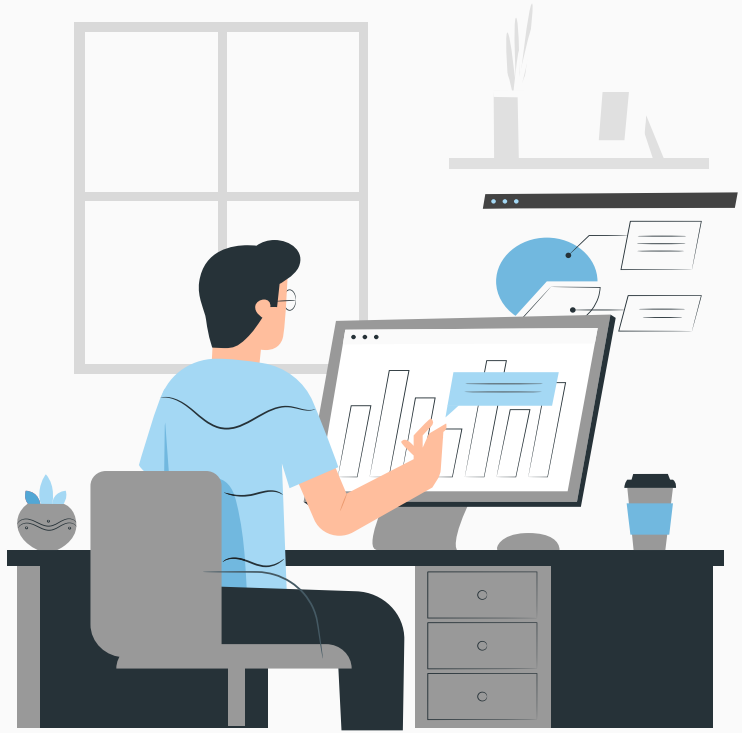
PENDING WORK

- Integrate IPFS with front end
- Integrate IPFS with Blockchain
- Implementing symmetric and asymmetric encryption

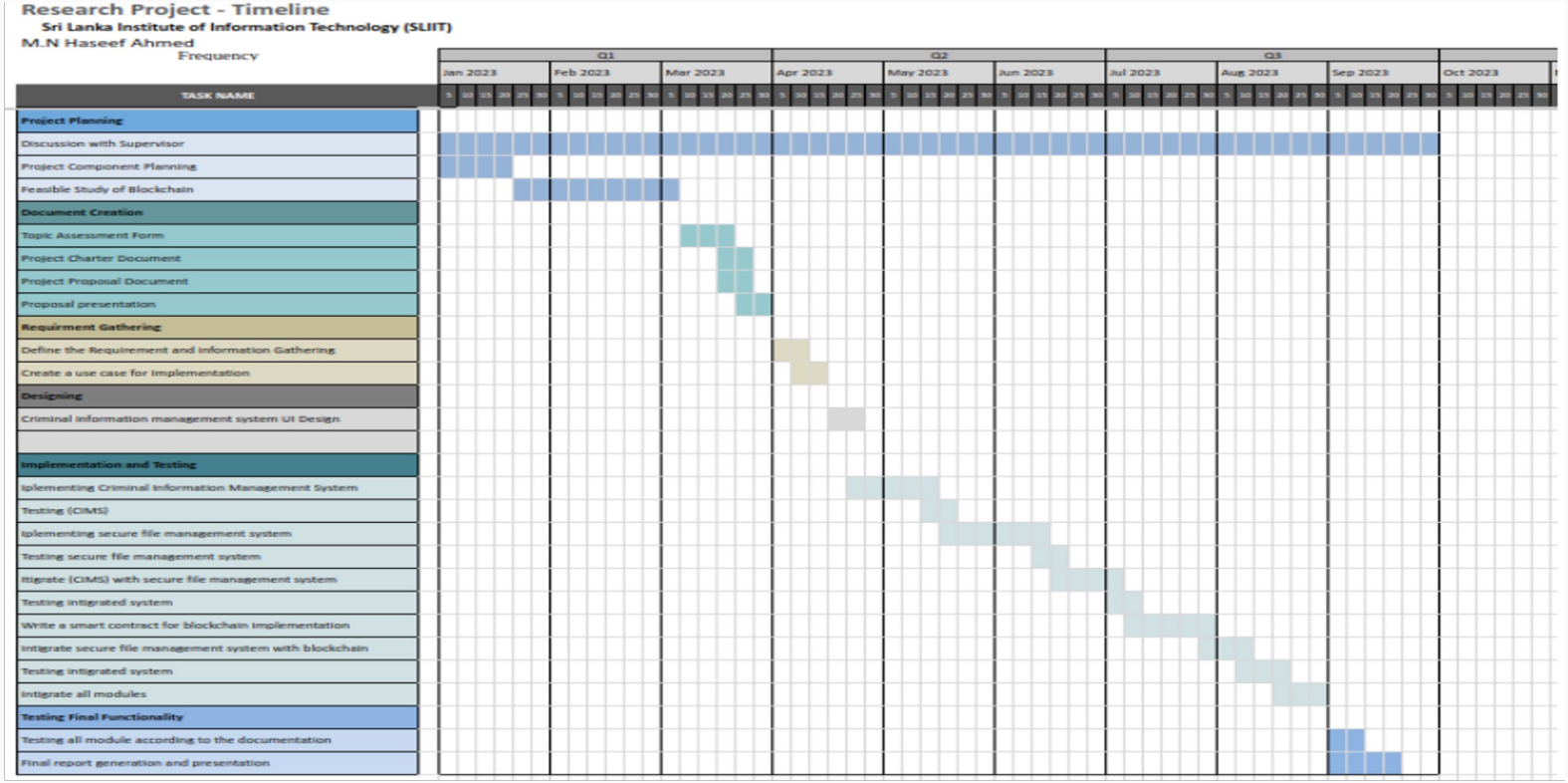


OTHER INFORMATION

1. GANTT CHART
2. SCHEDULE
3. REFERENCES



GANTT CHART


Research Project - Timeline
Sri Lanka Institute of Information Technology (SLIIT)
M.N Haseef Ahmed
Frequency
Q1
Q2
Q3
Jan 2023
Feb 2023
Mar 2023
Apr 2023
May 2023
Jun 2023
Jul 2023
Aug 2023
Sep 2023
Oct 2023
TASK NAME
Project Planning
Discussion with Supervisor
Project Component Planning
Feasible Study of Blockchain
Document Creation
Topic Assessment Form
Project Charter Document
Project Proposal Document
Proposal presentation
Requirment Gathering
Define the Requirement and Information Gathering
Create a use case for Implementation
Designing
Criminal Information management system UI Design
Implementation and Testing
Iplementing Criminal Information Management System
Testing (CIMS)
Iplementing secure file management system
Testing secure file management system
Itigrate (CIMS) with secure file management system
Testing intigrated system
Write a smart contract for blockchain implementation
Intigrate secure file management system with blockchain
Testing intigrated system
Intigrate all modules
Testing Final Functionality
Testing all module according to the documentation
Final report generation and presentation

SCHEDULE


M
T
W
T
F
S
S
Week 1
-
-
-
1
2
3
4
IMPLEMENTING CRYPTOGRAPHY
Week 2
5
6
7
8
9
10
11
FINAL EXAMS
Week 3
12
13
14
15
16
17
18
INTEGRATE FRONTEND WITH IPFS
Week 4
19
20
21
22
23
24
25
TESTING & BUG FIX
INTEGRATE IPFS WITH BLOCKCHAIN
Week 5
26
27
28
29
30
1
2
INTEGRATE IPFS WITH BLOCKCHAIN
TESTING & BUG FIX

REFERENCES

1.E. Onuiri, A. Oludele, O. Olufunmike and S. Oluwawunmi , "A REAL-TIME CRIME RECORDS MANAGEMENT SYSTEM FOR NATIONAL SECURITY AGENCIES," May 2015. [Online]. Available: https://www.researchgate.net/publication/305426207_A_REAL-TIME_CRIME_RECORDS_MANAGEMENT_SYSTEM_FOR_NATIONAL_SECURITY_AGENCIES. [Accessed 20 March 2023].

2.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.

3.S. Reno, S. Bhowmik and M. Ahmed, "Utilizing IPFS and Private Blockchain to Secure Forensic Information," 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), Rajshahi, Bangladesh, 2021, pp. 1-6, doi: 10.1109/ACMI53878.2021.9528180.

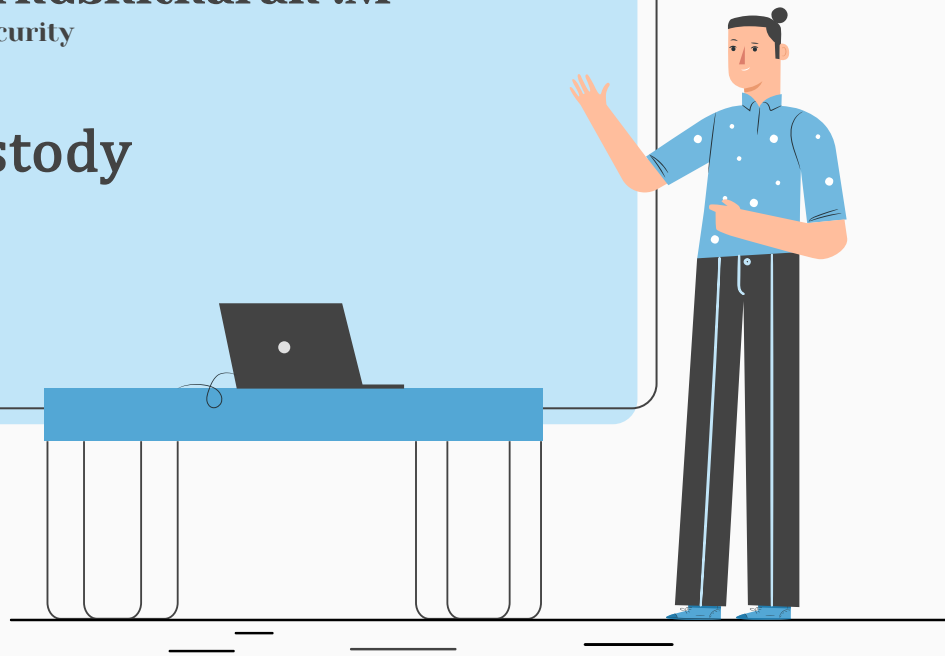
4.T.-S. C. J.-Y. W. Hsiao-Shan Huang, "A Secure File Sharing System Based on IPFS and Blockchain," 02 May 2022. [Online]. Available: https://arxiv.org/abs/2205.01728. [Accessed 20 March 2023]

5.D. Praveen, S. G. Totad, M. Rashinkar, R. Ostwal, S. Patil and P. M. Hadapad, "Scalable Blockchain Architecture using off-chain IPFS for Marks Card Validation," in *4th International Conference on Innovative Data Communication Technology and Application*, 2022.

IT19983370 | Thushitharan .M

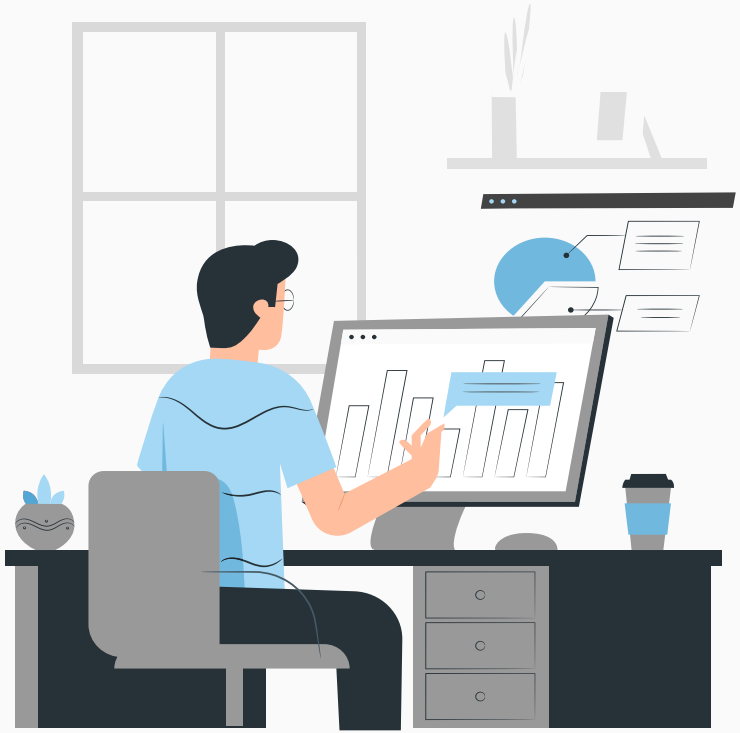
Specializing in Cyber Security

Chain of Custody



RESEARCH QUESTION

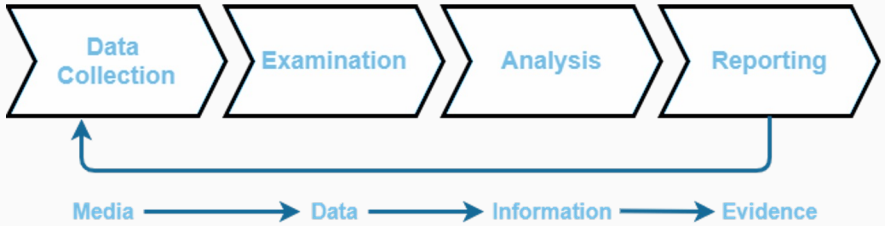
1. RESEARCH QUESTION
2. RESEARCH GAP
3. SUB OBJECTIVES



RESEARCH QUESTION

- **How can the implementation of chain of custody in blockchain increase the security of the criminal records management?**

- *Chain of custody is a logical sequence of keep the records of digital evidence process.*
- *Once peer uploads the file, the file is stored in a block including username, filesize and file data.*
- *These block gets appended to the current blockchain, which makes it impossible to edit or delete the file/block.*
- *The reason to implement file storing using blockchain is its ability to avoid any modification or deletion. No one can delete or corrupt our files that are stored.*



RESEARCH GAP

CONSIDERATION ON	EXISTING LOCAL DATABASE BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA	BLOCKCHAIN TECHNOLOGY FOR CRIMINAL INFORMATION MANAGEMENT SYSTEM
Security of Sensitive Criminal Records	MEDIUM	HIGH
Decentralization Of System	No	Yes
Ensure data Integrity	LOW	HIGH
Prevent loss of data	LOW	HIGH
Log Management	Easy	Hard
Confidentiality	LOW	HIGH

SPECIFIC OBJECTIVES

- Make the uploaded evidences immutable.
- Implement Evidence log management.
- Ensure Integrity, Availability.
- Increase the performance and usability of criminal Records.

SUB OBJECTIVES

- User friendly Interface
- Identify the stakeholders
- Recommendations and guidelines

SYSTEM DIAGRAM

Retrive the crime records for low enforcement

Police man

Login to the system

view the criminal records for investigation

Criminal information management System

Create a contract between the actors

(Smart contract + encryption)

Deploy the criminal records

Blockchain Approach

Crime Scene

Suspect/ Accused

Collecting Suspect / Criminal Evidence.

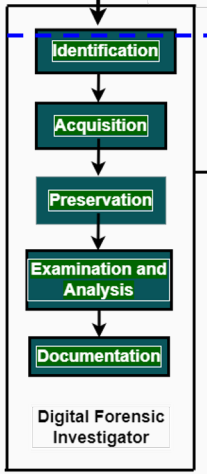
Field Officer

Evidence

Hand Over the Document to the Admin of Police

Admin of police department

Create, update, delete the criminal records



Digital Chain of custody

Chain of Custody

FUNCTIONAL REQUIREMENTS

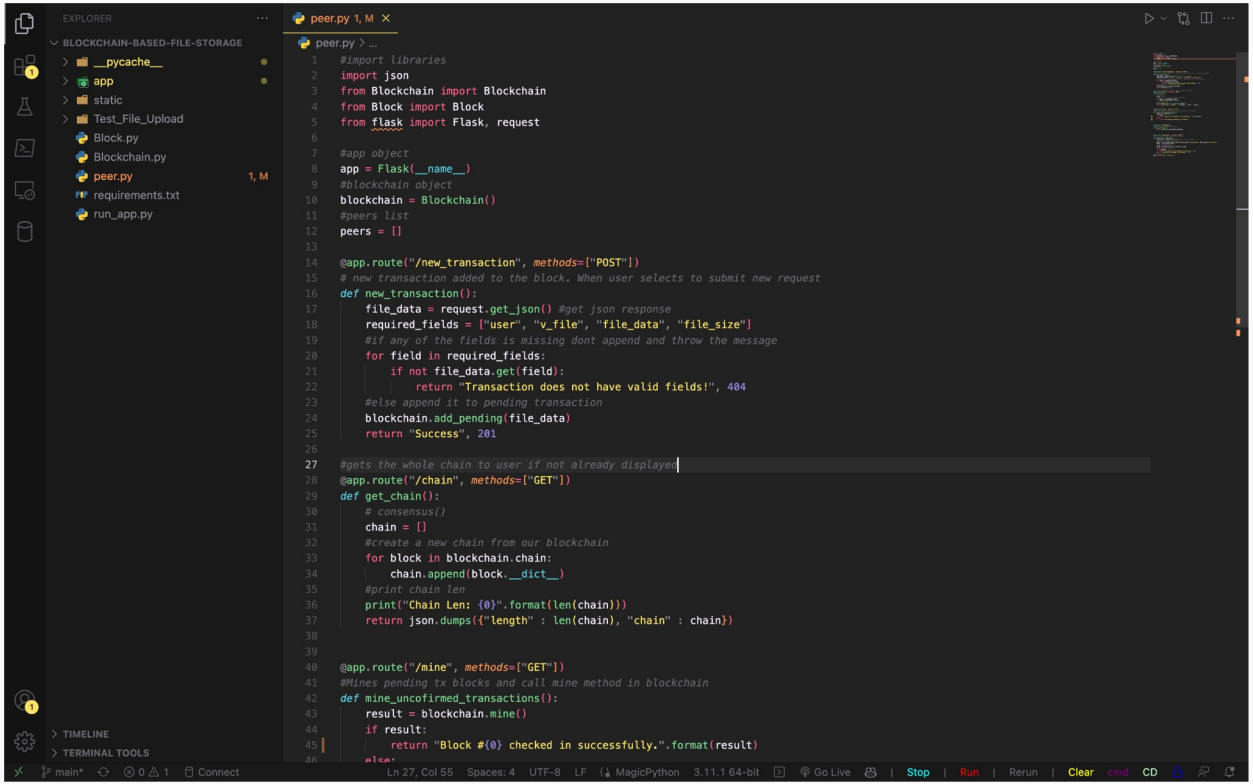
- Immutable Evidence Records
- Implement Evidence log management
- Integration with Criminal System.

NON – FUNCTIONAL REQUIREMENTS

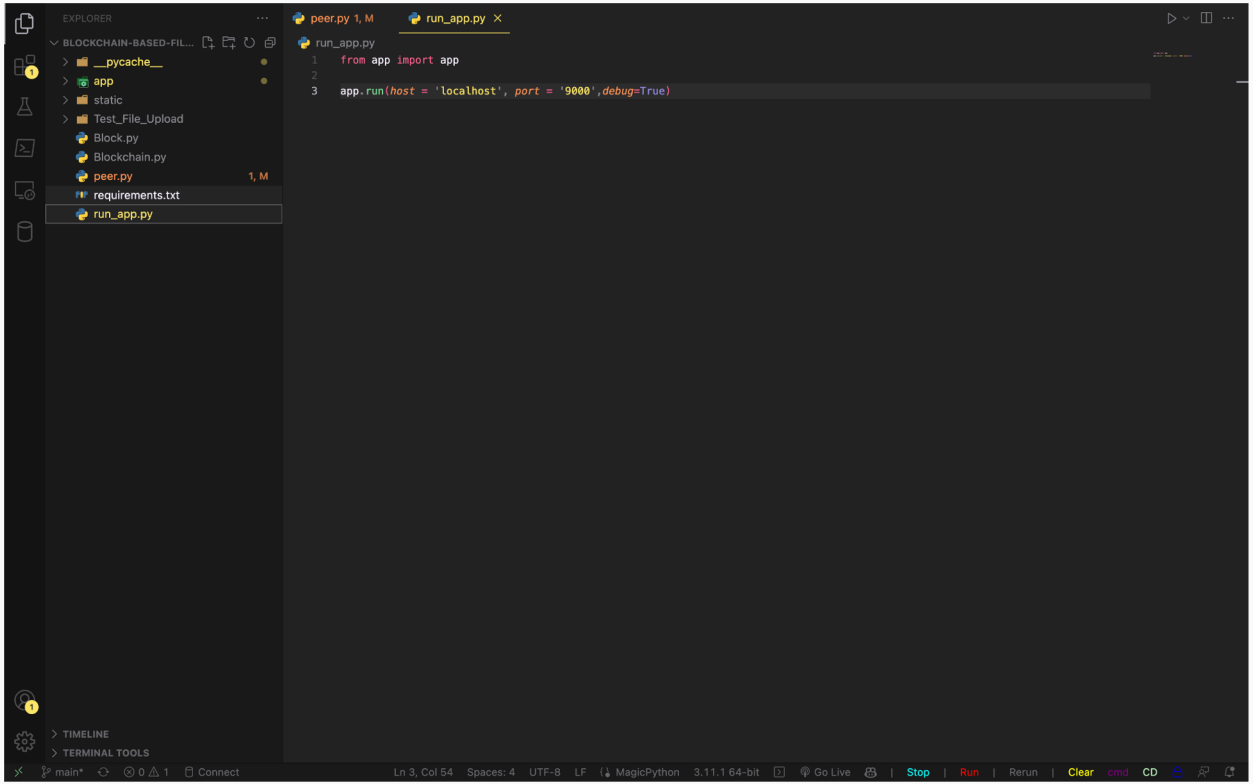
- Security
- User Friendly Interface
- Performance

IMPLEMENTATION

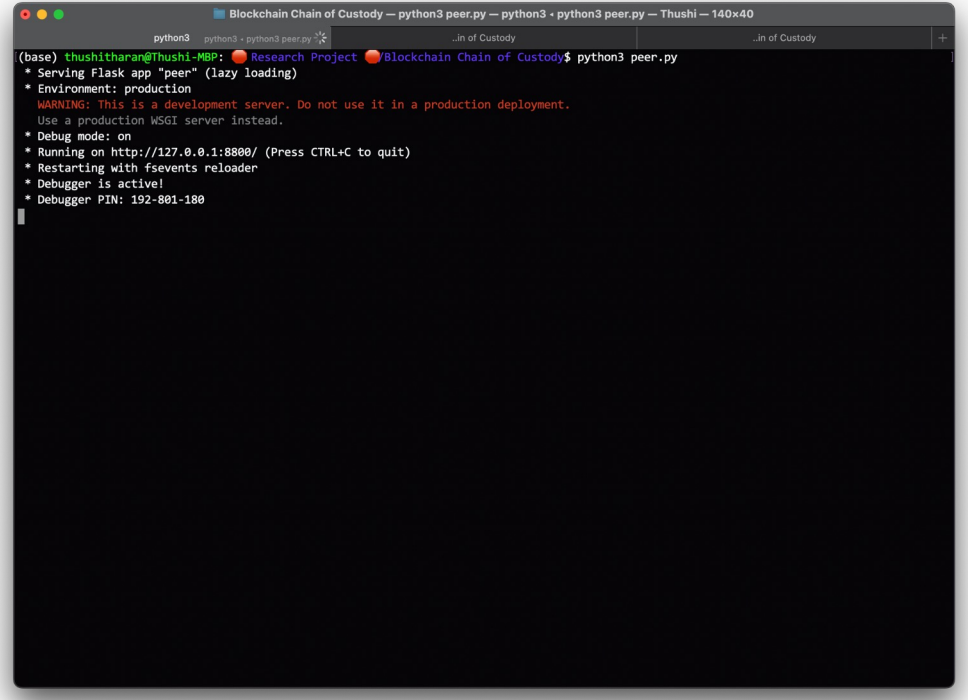
Peer Code


EXPLORER
BLOCKCHAIN-BASED-FILE-STORAGE
__pycache__
app
static
Test_File_Upload
Block.py
Blockchain.py
peer.py 1, M
requirements.txt
run_app.py
peer.py 1, M
peer.py > ...
#import libraries
import json
from Blockchain import Blockchain
from Block import Block
from flask import Flask, request
#app object
app = Flask(__name__)
#blockchain object
blockchain = Blockchain()
#peers list
peers = []
@app.route("/new_transaction", methods=["POST"])
# new transaction added to the block. When user selects to submit new request
def new_transaction():
file_data = request.get_json() #get json response
required_fields = ["user", "v_file", "file_data", "file_size"]
#if any of the fields is missing dont append and throw the message
for field in required_fields:
if not file_data.get(field):
return "Transaction does not have valid fields!", 404
#else append it to pending transaction
blockchain.add_pending(file_data)
return "Success", 201
#gets the whole chain to user if not already displayed
@app.route("/chain", methods=["GET"])
def get_chain():
# consensus()
chain = []
#create a new chain from our blockchain
for block in blockchain.chain:
chain.append(block.__dict__)
#print chain len
print("Chain Len: {0}".format(len(chain)))
return json.dumps({"length" : len(chain), "chain" : chain})
@app.route("/mine", methods=["GET"])
#Mines pending tx blocks and call mine method in blockchain
def mine_uncofirmed_transactions():
result = blockchain.mine()
if result:
return "Block #{0} checked in successfully.".format(result)
else:
TIMELINE
TERMINAL TOOLS
main*
0 1
Connect
Ln 27, Col 55
Spaces: 4
UTF-8
LF
MagicPython
3.11.1 64-bit
Go Live
Stop
Run
Rerun
Clear
cmd
CD

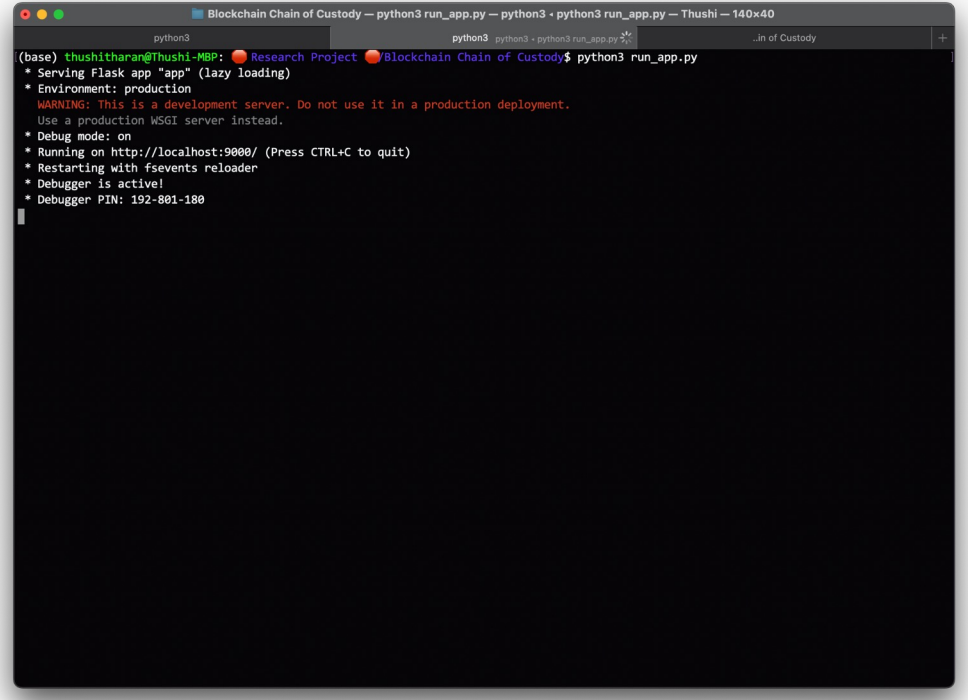
Python code to run the application in web browser



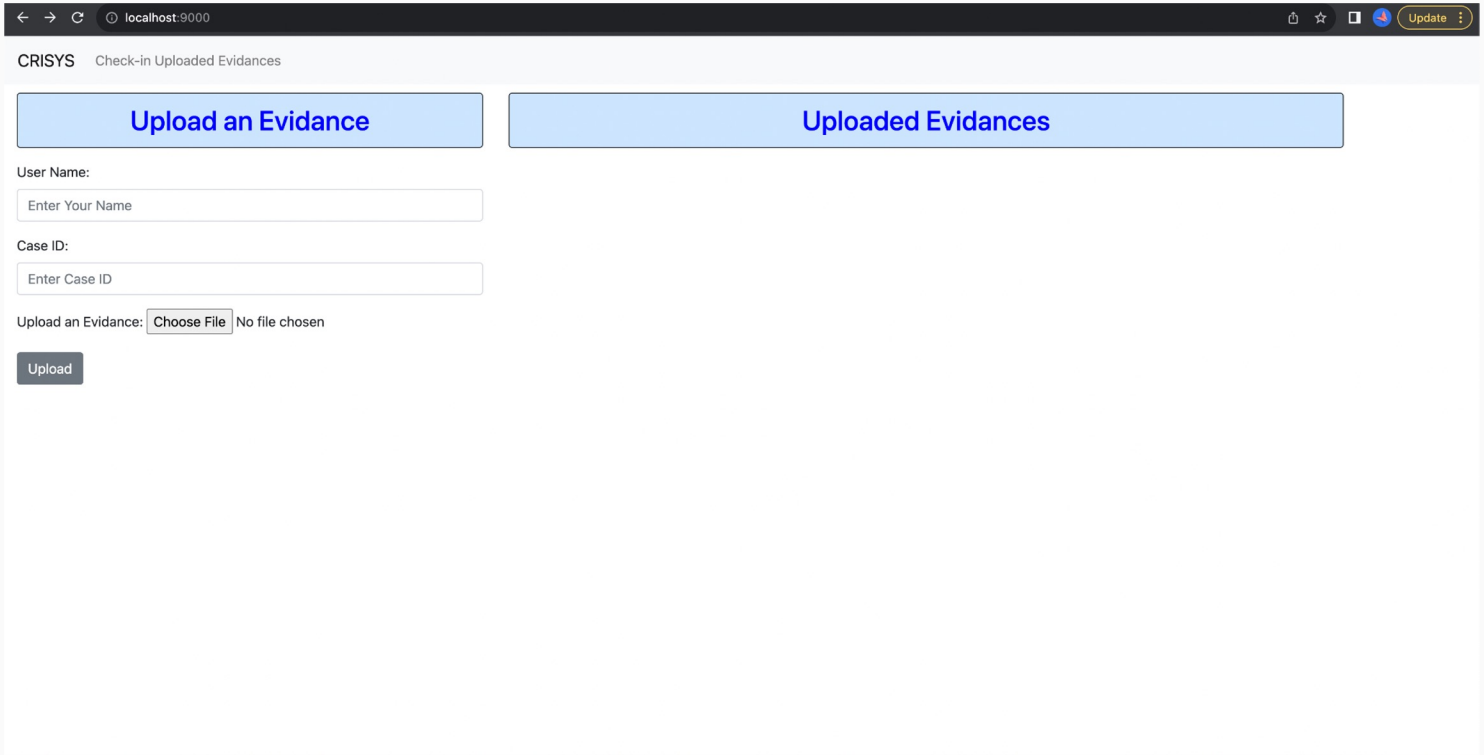
Run the peer.py file



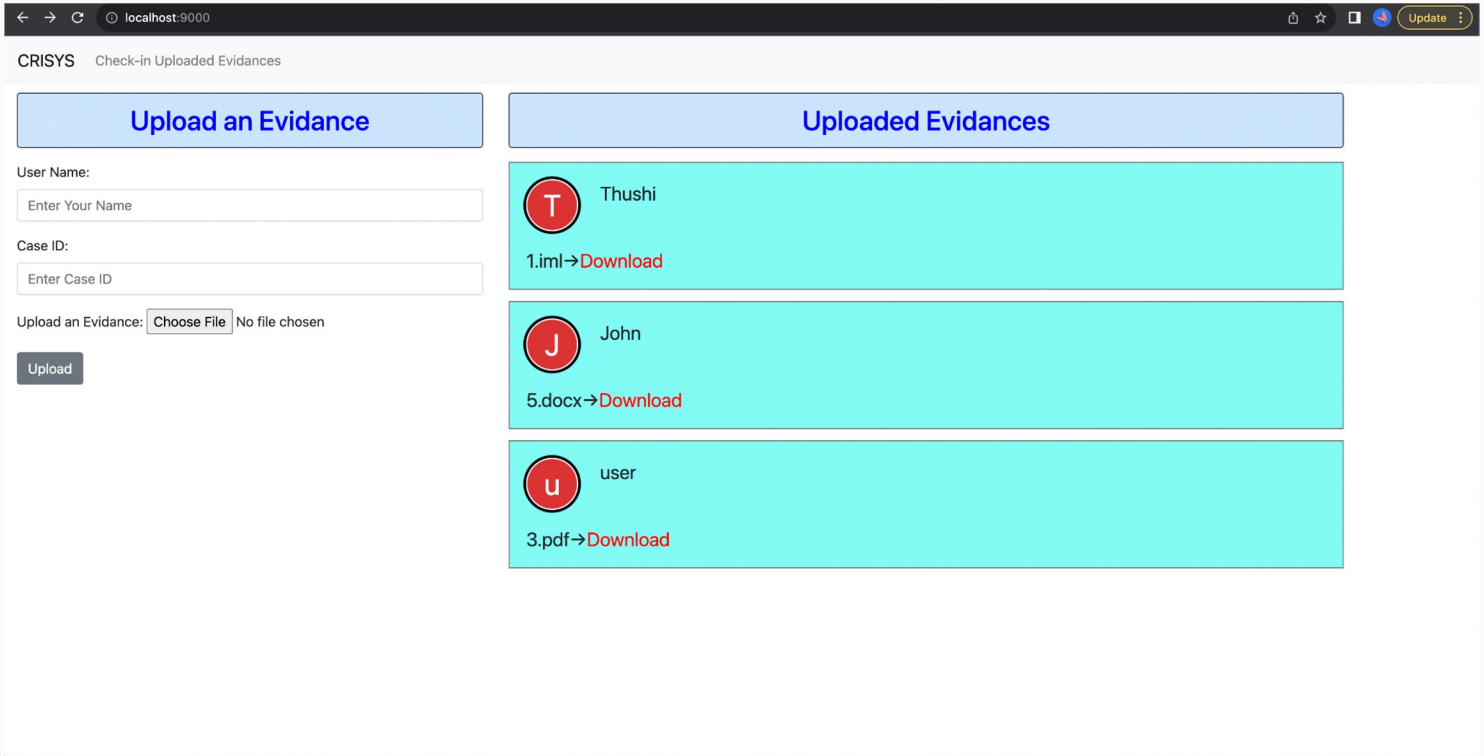
Run the peer.py file



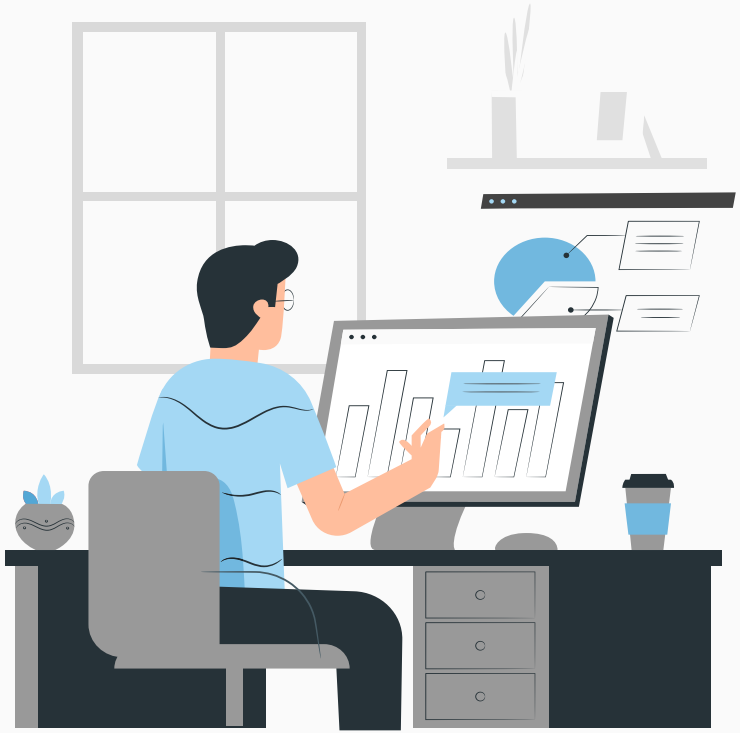
Webview before upload the evidences



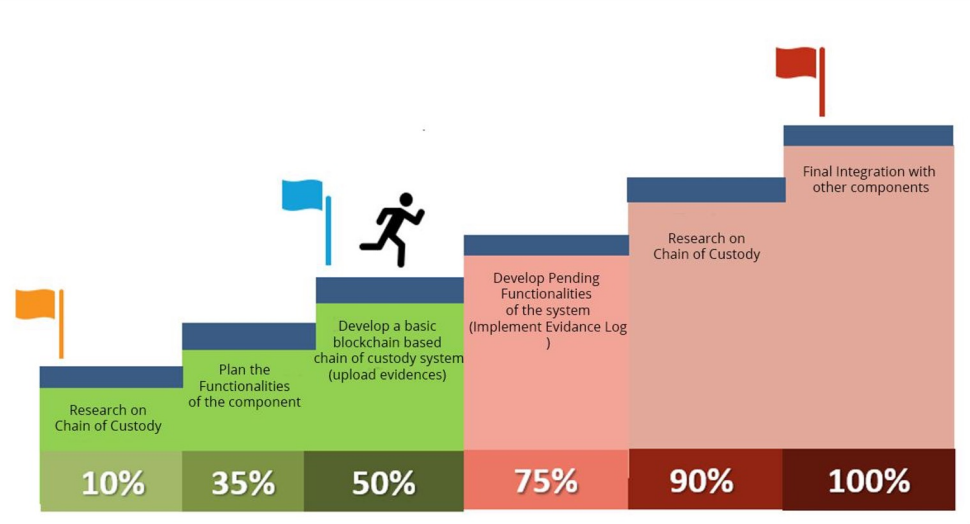
Web view after upload the evidences

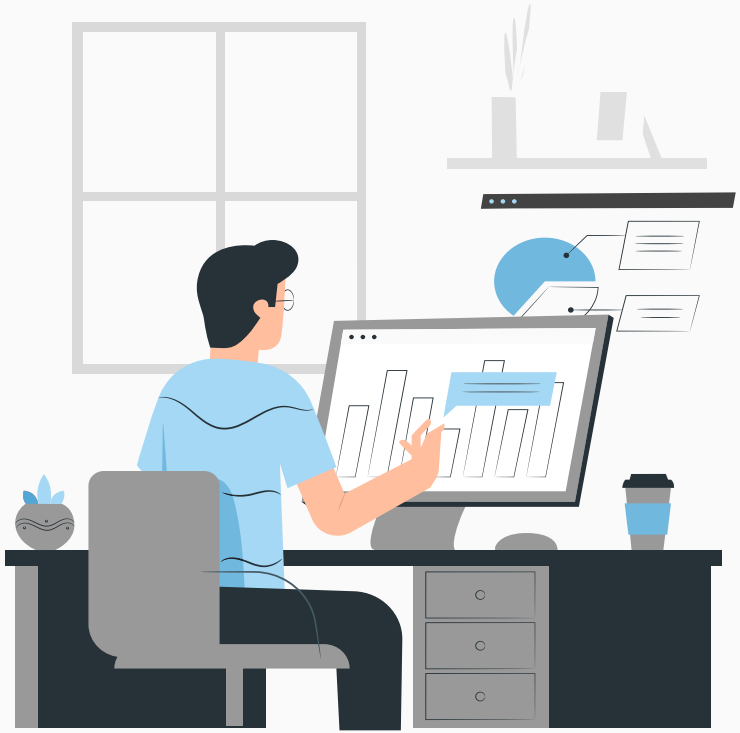


Demonstration



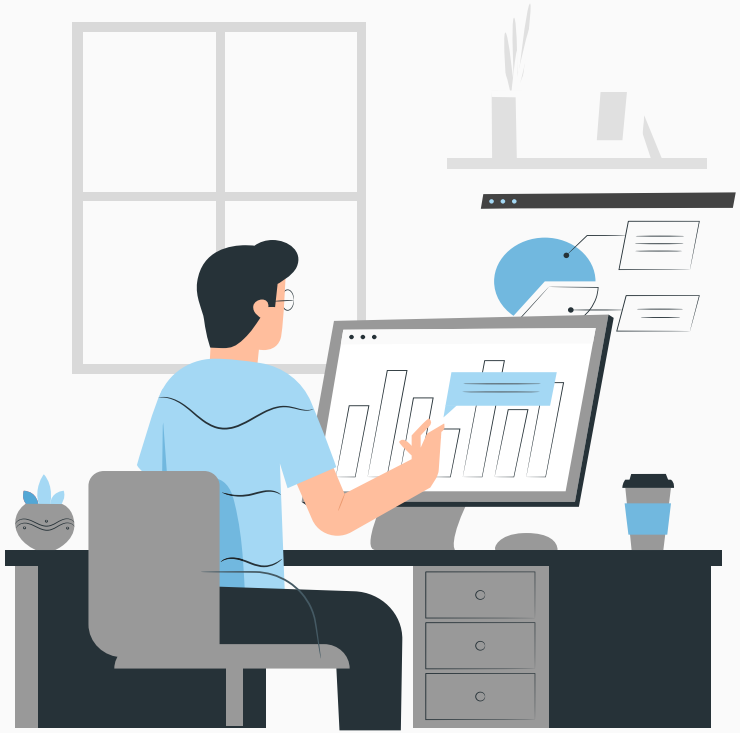
PENDING WORK



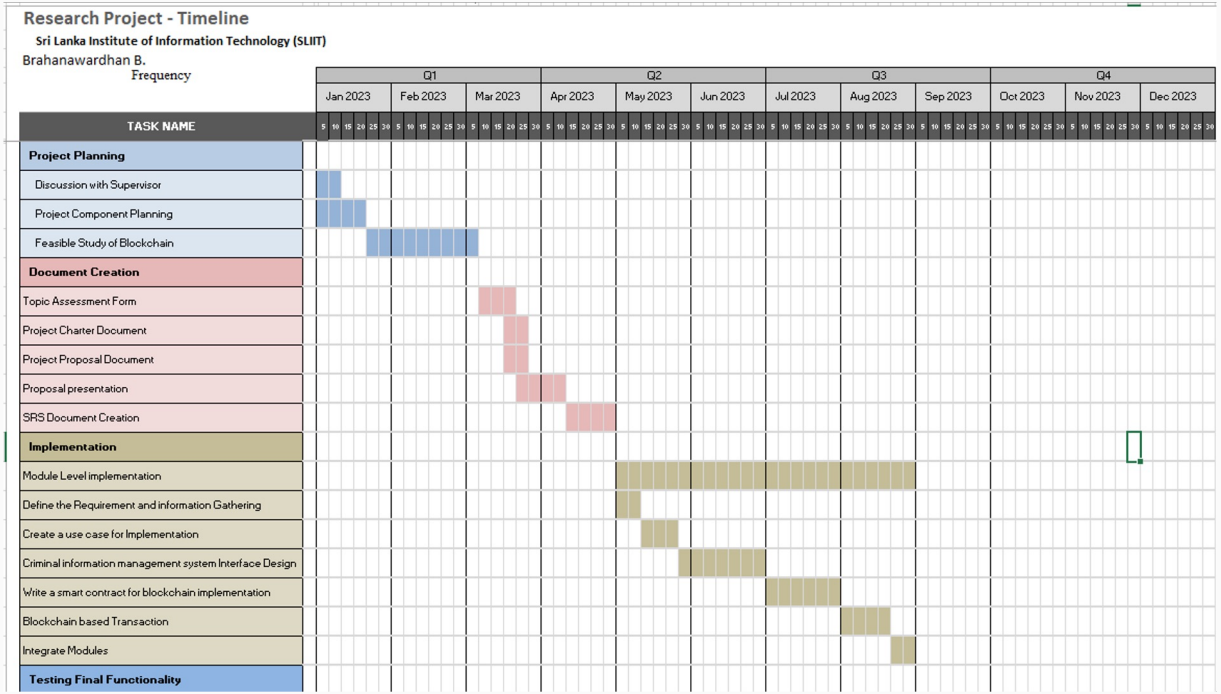


PENDING WORK

- Add evidence verification functionality through blockchain.
- Add evidence log management.
- Integrate the evidence details with the respective case.
- Integrate with the other components



GANTT CHART


Research Project - Timeline
Sri Lanka Institute of Information Technology (SLIIT)
Brahanawardhan B.
Frequency
Q1
Q2
Q3
Q4
Jan 2023
Feb 2023
Mar 2023
Apr 2023
May 2023
Jun 2023
Jul 2023
Aug 2023
Sep 2023
Oct 2023
Nov 2023
Dec 2023
TASK NAME
Project Planning
Discussion with Supervisor
Project Component Planning
Feasible Study of Blockchain
Document Creation
Topic Assessment Form
Project Charter Document
Project Proposal Document
Proposal presentation
SRS Document Creation
Implementation
Module Level implementation
Define the Requirement and information Gathering
Create a use case for Implementation
Criminal information management system Interface Design
Write a smart contract for blockchain implementation
Blockchain based Transaction
Integrate Modules
Testing Final Functionality

REFERENCES

1. Prayudi, Yudi & Sn, Azhari. (2015). Digital Chain of Custody: State of The Art. International Journal of Computer Applications. 114. 975-8887. 10.5120/19971-1856..

1. Anderson, G.S., Litzenberger, R. and Plecas, D. (2002), "Physical evidence of police officer stress", Policing: An International Journal, Vol. 25 No. 2, pp. 399-420.

1. Tasnim, Maisha & Omar, Abdullah & Rahman, Shahriar & Bhuiyan, Md. (2018). CRAB: Blockchain Based Criminal Record Management System. 294-303. 10.1007/978-3-030-05345-1_25.

THANK YOU!

Project Details;

Project ID: 23-270

Supervisor: Mr. Kanishka Yapa

Co-Supervisor: Ms. Dinithi Pandithage

Group Details;

IT20150952 - Brahanawardhan B

IT20171438 - Wijayarathne S. N

IT20157814 - Ahmed M. N. H

IT19983370 - Thushitharan M.