BLOCKCHAIN-BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM

IN SRI LANKA

GROUP ID: TMP-23-270

SLIIT
FACULTY OF COMPUTING

TABLE OF CONTENT

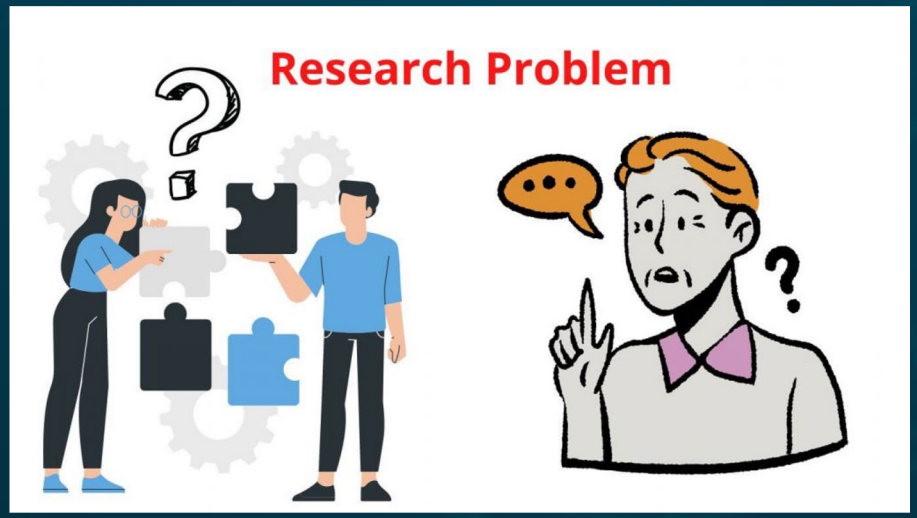
OVERALL PROJECT DESCRIPTION

Project Details;

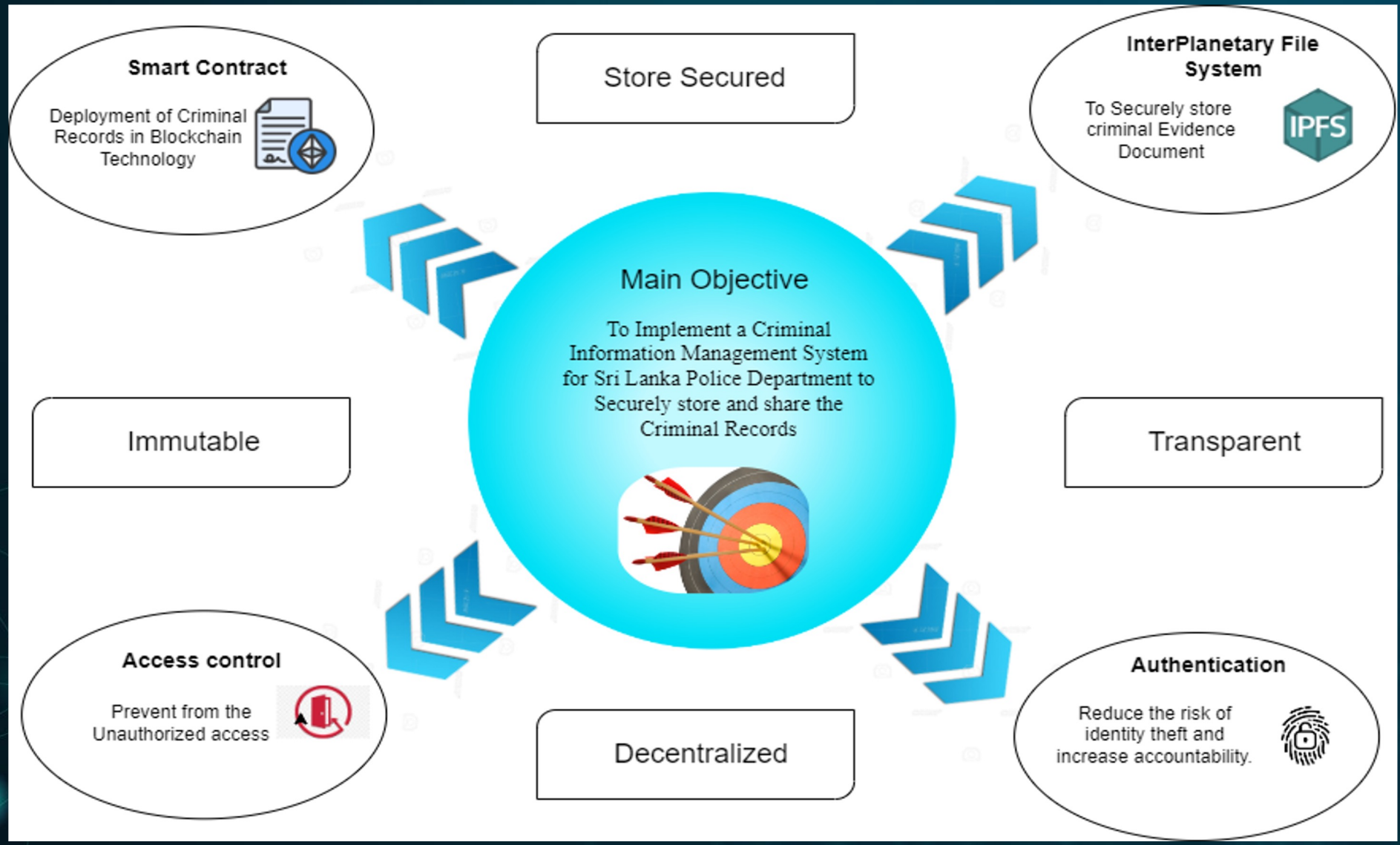
- Project ID: TMP-23-270
- Supervisor: Mr. Kanishka Yapa
- Co-Supervisor: Ms. Dinithi Pandithage

RESEARCH PROBLEM

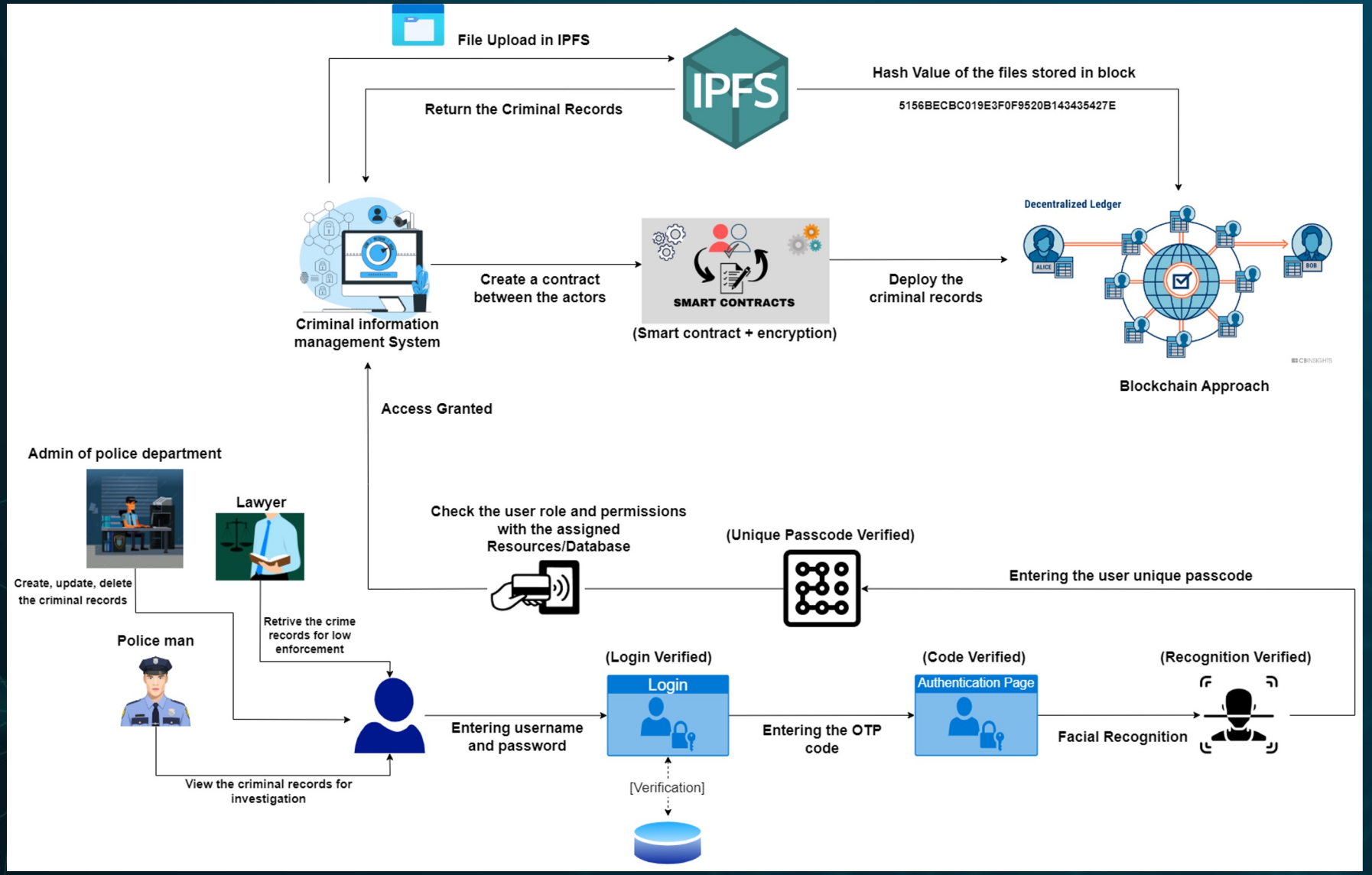
- Lack of integration
- Inconsistent data quality
- Privacy and Security Concern
- Insufficient Process
- Lack of transparency



OBJECTIVES


Smart Contract
Deployment of Criminal Records in Blockchain Technology
Store Secured
InterPlanetary File System
To Securely store criminal Evidence Document
IPFS
Main Objective
To Implement a Criminal Information Management System for Sri Lanka Police Department to Securely store and share the Criminal Records
Immutable
Transparent
Access control
Prevent from the Unauthorized access
Decentralized
Authentication
Reduce the risk of identity theft and increase accountability.

OVERALL SYSTEM DIAGRAM



IT20150952 | BRAHANAWARDHAN B.

Student's Specialization - Cyber Security

INTRODUCTION

IMPLEMENTING SMART CONTRACT IN CRIMINAL INFORMATION MANAGEMENT USING BLOCKCHAIN TECHNOLOGY

- Current state of criminal information Management system in Sri Lanka.
- Introducing Blockchain technology in our Criminal Information Management system in Sri Lanka.
- Key features and benefits of blockchain based criminal information management system.
  - Immutable records
  - Efficiency of criminal Records
  - Data Privacy
  - Ensure Confidentiality, Availability and Integrity.

RESEARCH PROBLEM

RESEARCH GAP

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

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 ?

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.

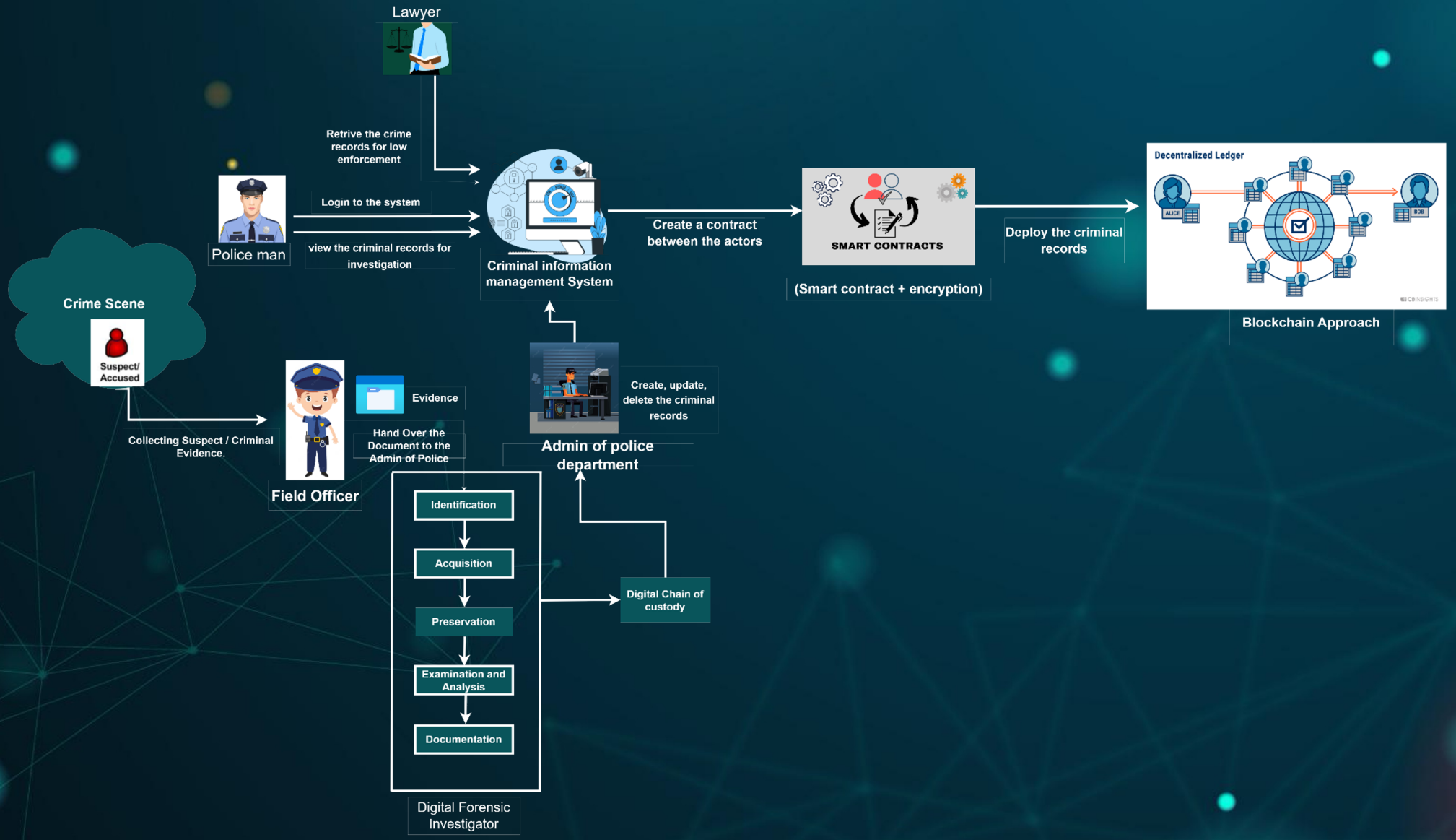
SUB OBJECTIVES

- 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

- Research Design
- Data Collection: Collecting Criminal Records
- Blockchain technology Evaluation
- Smart contract Design
- Legal and Regulatory Framework Evaluation.
- Implementation

SYSTEM OVERVIEW DIAGRAM



REFERENCES

- IT20150952 | BRAHANAWARDHAN B.

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

[2] “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].

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

[4] 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.

Student's Specialization - Cyber Security

RESEARCH QUESTION

- **HOW TO SECURE SYSTEM LOGIN BY IMPLEMENTING A SECURE AUTHENTICATION SYSTEM TO THE BLOCKCHAIN-BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA?**

- Every system and application requires a user account.
  - Username
  - Password

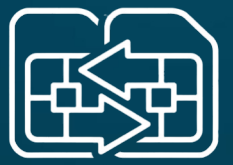
  } 1FA (1st Factor)
- Technological Improvement;
  - Brute Force Attacks
  - Phishing Attacks
  - Social Engineering Attacks
  - Etc.



- As an additional layer; **Two-Factor Authentication System (2FA)** was introduced.

2FA SECURE? Can 2FA be HACKED?

- SIM Swapping
  - Security analysis of SMS as a second factor of authentication [1].
- SIM Cloning
  - A novel Two-Factor HoneyToken Authentication Mechanism [2].
- Man-in-the-Middle Attacks
  - How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication [3].
- Phishing Attacks
  - How to Attack Two-Factor Authentication Internet Banking [4].



- As a solution and an additional layer of security: Inherence Factor Authentication
  - Fingerprint
  - Facial Recognition
  - Voice Recognition

} 3FA (3rd Factor)

RESEARCH GAP

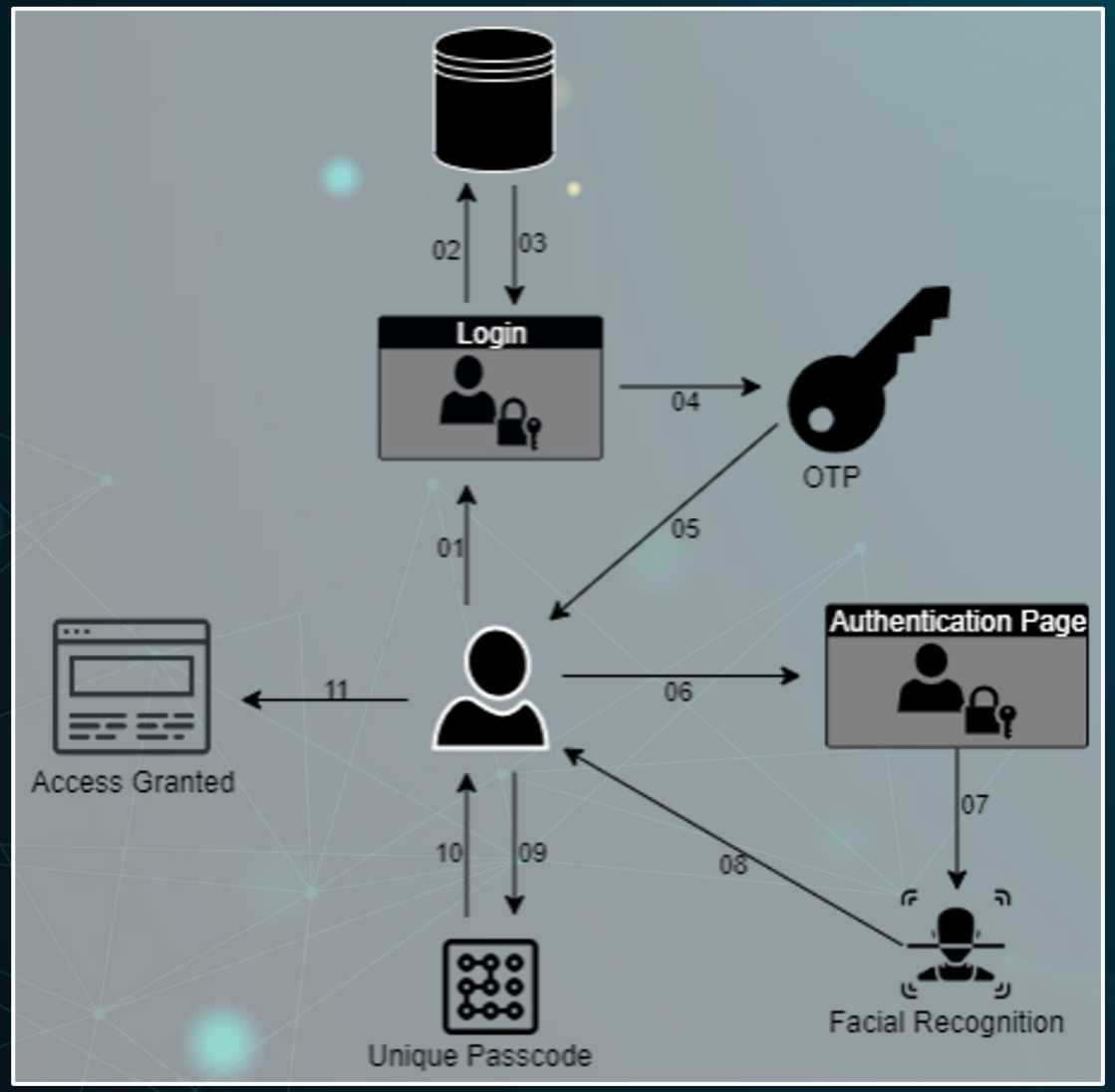
CONSIDERATION ON	EXISTING SYSTEMS	PROPOSED SYSTEM
1ST FACTOR	Security Level is **LOW**	Security Level is **HIGH**
2ND FACTOR	Security Level is **MODERATE**	Security Level is **HIGH**
3RD FACTOR	Security Level is **MODERATE**	Security Level is **HIGH**
CONFIDENTIALITY	Security Level is **LOW**	Security 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 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

SYSTEM OVERVIEW 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

METHODOLOGY

- 1st Factor;
  - Highest-level of Security Standards
  - Alerts Generated
  - Number of Attempts
- 2nd Factor;
  - 6-Digit Code → 6-Character Code [59,049 → 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

REFERENCES

- **IT20171438 | WIJAYARATHNE S. N.**

1. 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
2. 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.
3. 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
4. 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 | AHMED M. N. H.

Student's Specialization - Cyber Security

INTRODUCTION

SECURE FILE MANAGEMENT SYSTEM IN DECENTRALIZED NETWORK

- In criminal information management system most challenging part is managing information securely
  - Confidentiality
  - Integrity
  - Availability

- Criminal Information Management System need to handle massive amount of files
  - Video,Audio,Images,Documents and,Etc.

RESEARCH PROBLEM

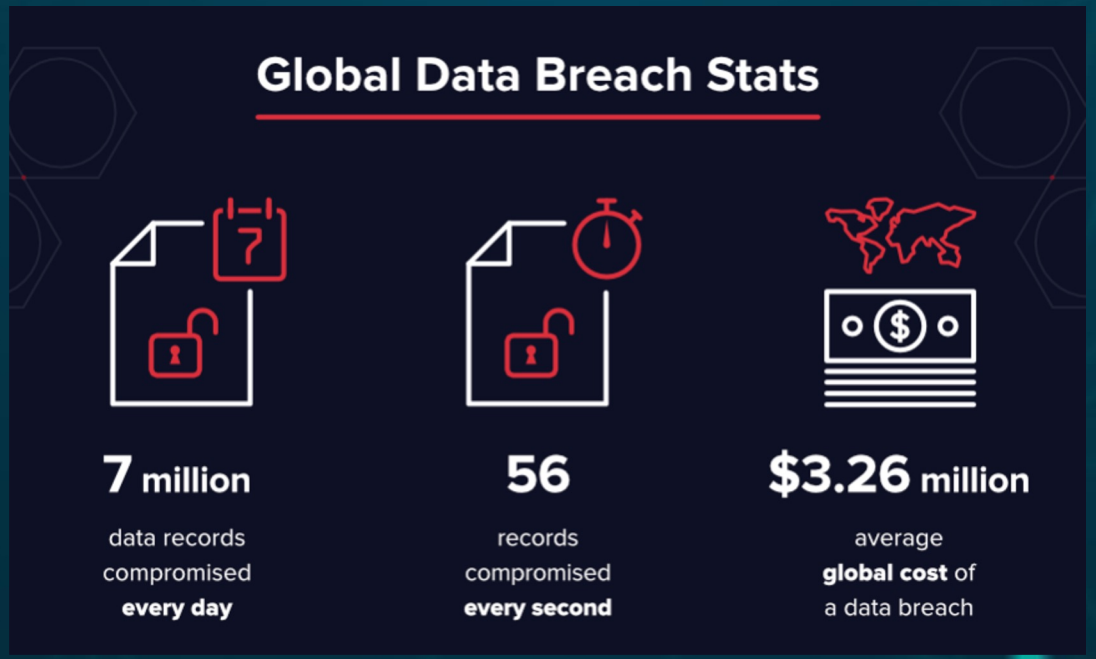
- Manual file sharing system
  - Paper based
  - Store files in cupboard and etc

- Centralize System
  - Sorting files in a single database without proper encryption

RESEARCH PROBLEM

- Data Breach

- Vulnerabilities in Current file management system
  - SQL Injection Attack
  - DDoS Attack
  - Theft / Stolen of the Files



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 OBJECTIVES

Propose Secure File Management System in Decentralized Network

- To provide secure storage platform for criminal information management system
- To ensure confidentiality, integrity, availability of the information

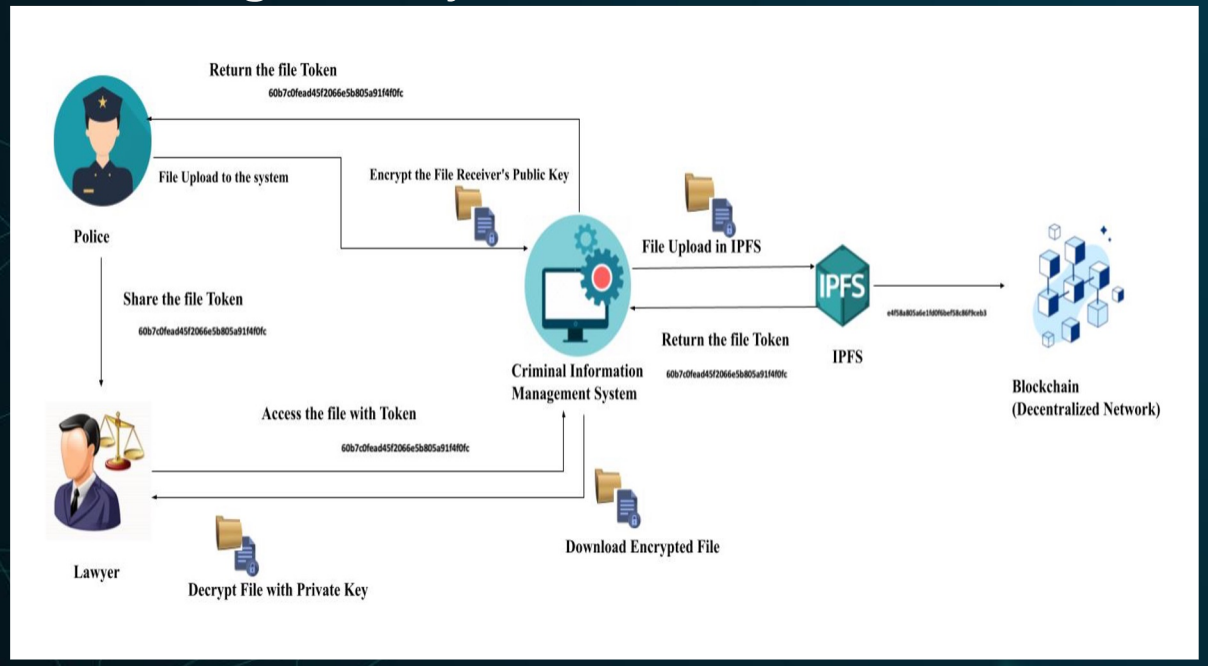
SUB OBJECTIVES

- Implementing cryptography secure file management system to share file

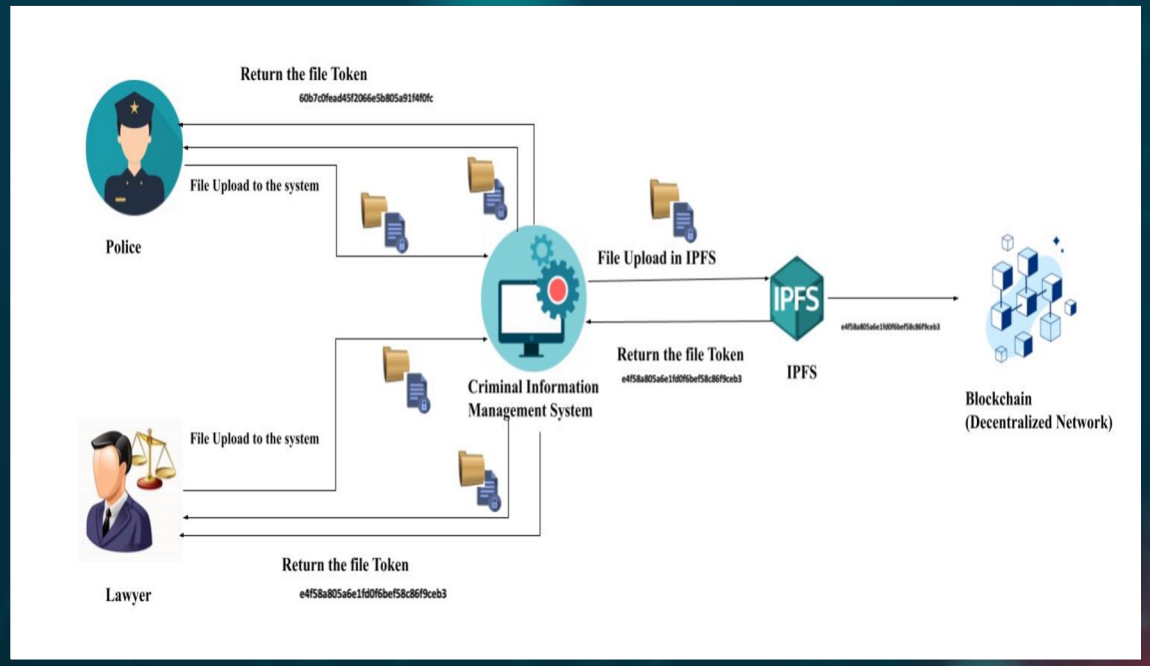
- Implementing cryptography secure file management system to store file

SYSTEM DIAGRAM

1. Implementing cryptography secure file management system to share file



2. Implementing cryptography secure file management system to store file



METHODOLOGY

- Implementing,
  - criminal information management system
  - Secure file management system
  - Additional layer with cryptography to secure file management
  - Integrating secure file management system with blockchain

REFERENCES

- IT20157814 | AHMED M. N. H.

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.

Student's Specialization - Cyber Security

INTRODUCTION

PERMISSION BASED ACCESS CONTROL FOR BLOCKCHAIN BASED SYSTEMS

- Importance of access control.
- Current access control methods following in Sri Lanka - Manual Paper-based
- Current access control methods following internationally - Digitized but not a controlled access
- Base idea behind this - Corruption prevention

RESEARCH PROBLEM

- Corruption status in Sri Lanka
- Corruption faced by the Department of Police Sri Lanka
- Criminals contribution to the corruption
- Consequences of the corruption
- Corruption scenario and Explanation - If a criminal can corrupt an officer in the police department, that officer can destroy or manipulate the documents/records/evidences as per the criminal's preference. No matter that he/she is a high level or low level officer.

RESEARCH GAP

- Existing Access control method in Sri Lanka and Internationally - Paper Based/uncontrolled access control/physical access control
- Problems in existing access control
  - Anyone in the department can manipulate/delete the criminal/crime records
  - Anyone can add criminal records without verifying it, destroy the paper based evidences, destroy complaint letters/FIR files. This leads to integrity violation.

SPECIFIC OBJECTIVES

Propose a permission based Access control

- To prevent access control violations, we are proposing a permission based access control.
- This is using CRUD operations.
- To ensure confidentiality, integrity.
- Prevent corruption level within the department.

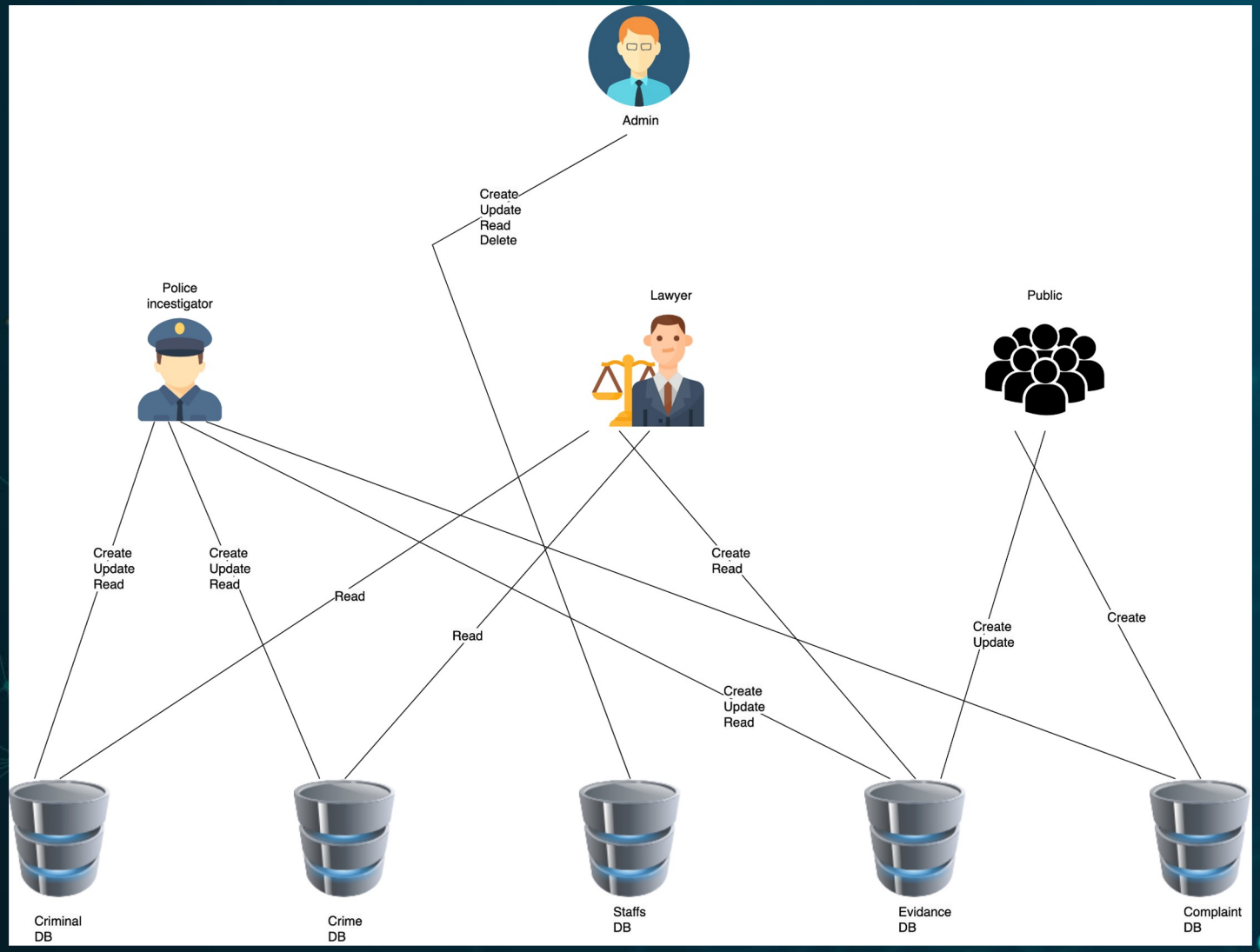
SUB OBJECTIVES

- Implementing log monitoring facility.
- Better and easy User Interface for admin dashboard
- Reducing Physical storage by digitizing all paper works.
- Generating Reports(crime, criminal)

METHODOLOGY

1. Defining Roles, Permissions
2. Grant/Revoke permissions
3. Implement Log monitoring system to monitor unauthorized access activities.

COMPONENT OVERVIEW DIAGRAM

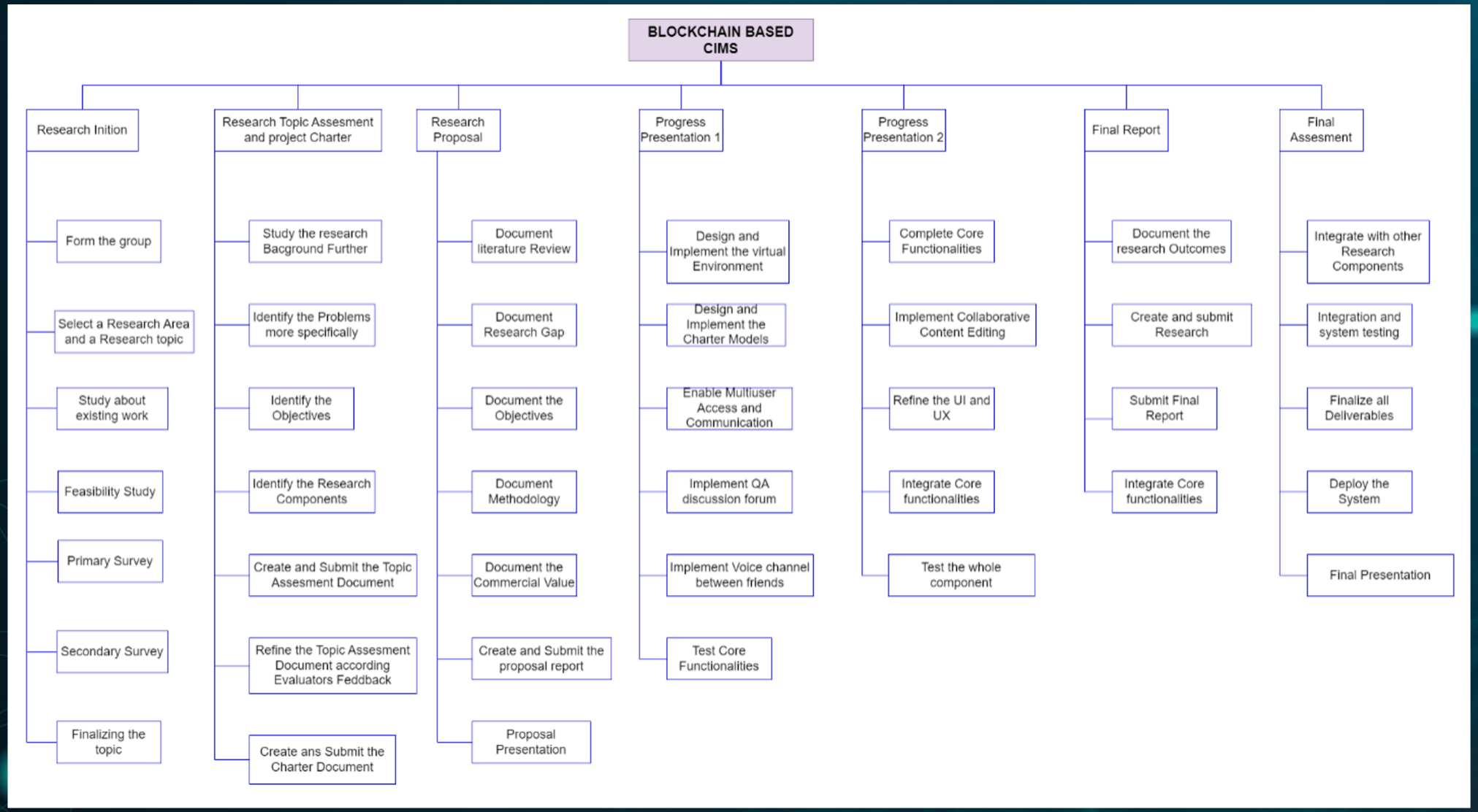


REFERENCES

- IT19983370 | THUSHITHARAN M.

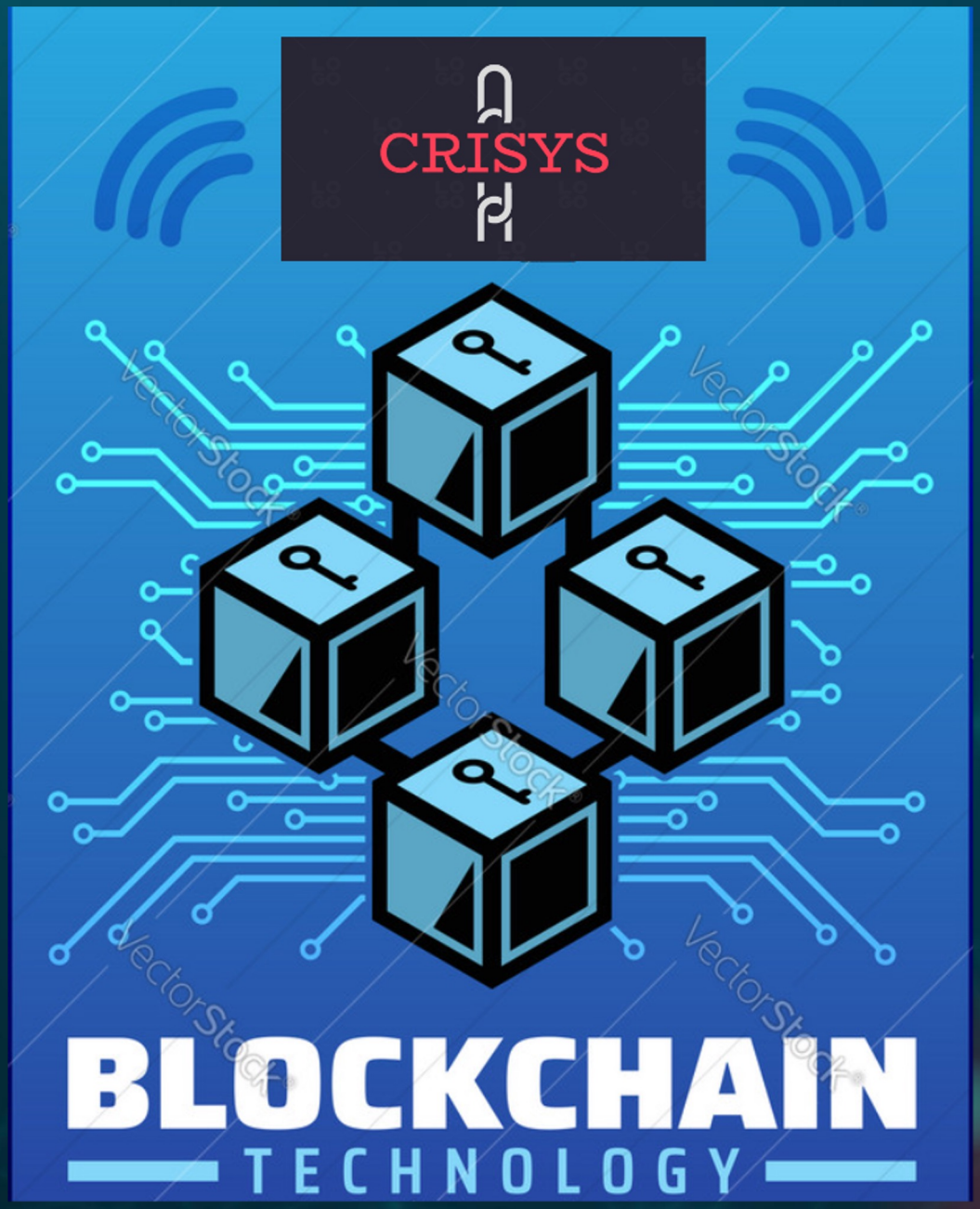
1. Onuiri, Ernest & Oludele, Awodele & A, Olaore & O, Sowunmi & A., Ugo-Ezeaba. (2015). A REAL-TIME CRIME RECORDS MANAGEMENT SYSTEM FOR NATIONAL SECURITY AGENCIES. European Journal of Computer Science and Information Technology.
2. K. Yapa, A. N. Senaratne, R. P. D. T. D. Pathirathna, Y. P. C. N. Priyamantha, W. D. S. Dias and B. Katukithulgala, "Improve the Efficiency and Security by Digitalizing the Sri Lankan Police Department," 2021 3rd International Conference on Advancements in Computing (ICAC), Colombo, Sri Lanka, 2021, pp. 37-42, doi: 10.1109/ICAC54203.2021.9671175.
3. Cooray, N.A.C. and Weerasinghe, K.G.H.D. 2016. Crime Information Management System for Sri Lanka Police. 1st International Conference on Library and Information Management (ICLIM - 2016), 21st - 22nd October 2016, Department of Library and Information Science, Faculty of Social Sciences, University of Kelaniya, Sri Lanka. p 17-18.

WORK BREAKDOWN FLOW



COMMERCIALIZATION

- Target Market (Suitable market only)
  - Law enforcement agencies
  - Private investigators
  - Police department
- Method Of Profit
  - Under our maintenance services.
  - Profit gain from Monthly charges.
- Provide customer Support.



THANK YOU!

Project Details;

- Project ID: TMP-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.