IT4010 – Research Project - 2023

Topic Assessment Form

Project ID: TMP-23-270

1. Topic (12 words max)

Blockchain Based Criminal Information Management System in Sri Lanka

2. Research group the project belongs to

Computing Infrastructure and Security (CIS)

3. Research area the project belongs to

Cyber Security (CS)

4. If a continuation of a previous project:

Project ID	
Year	

5. Team member details

Student Name	Student ID	Specialization
Leader: Brahanawardhan B	IT20150952	CS
Member 2: Wijayarathne S. N	IT20171438	CS
Member 3: Thushitharan M	IT19983370	CS
Member 4: Ahmed M.N.H	IT20157814	CS

6. Brief description of the research problem including references (200 – 300 words max)

The increasing number of criminal activities has led to a need for a more efficient and secure system for managing criminal information. According to our analysis, Major problem in our country is maintaining criminal information records in paper basis and one of the key challenges facing the current criminal information management system is the lack of transparency, security, and immutability in the storage and dissemination of information. This has led to numerous data breaches and unauthorized data modification causing significant damage to both individuals, organizations, and government. Blockchain technology has the potential to provide a secure and transparent solution for criminal information management. A blockchain based criminal information management system can use decentralized ledgers to store criminal records, ensuring that the information is secure and tamper-proof. The use of smart contracts can also automate the process of updating and accessing the information, reducing the potential for human error.

This system can also provide a secure and transparent platform for sharing criminal information between law enforcement agencies and other relevant. Stakeholders, improving collaboration and coordination in the fight against crime. In conclusion, a blockchain based criminal information management system is a promising solution for improving the efficiency, security, and transparency of criminal information management. This research will contribute to the development of a secure and efficient platform for managing criminal information using Blockchain technology, which can have a significant impact on the criminal justice system and the fight against crime.

Sub Problem (Member 01) – criminal information management system is existing with centralized database approach and transparent of criminal records.

Criminal information management system is developed in centralized database manner, and it consists following problem,

- Interoperability problem when identifying criminals in criminal information management system.
- Lack of consistency when identifying Criminals
- Lack of standards for sending, receiving, and managing information between criminal record management system.
- The lack of shared data in criminal record management system.

Privacy and Security: while blockchain technology is inherently secure, the public nature of blockchain networks can make it difficult to keep certain data private such as criminal records. In some cases, hackers have been able to exploit vulnerabilities in blockchain networks to steal criminal records or altering criminal records.

References:

1. F. J. BARROW, "Criminal Record Management System In the Perspective of Somalia," www.grin.com, 2019. https://www.grin.com/document/491032.

2. Maisha A. Tasnim et al., "CRAB: Blockchain Based Criminal Record Management System", SpaCCS, LNCS 11342, pp. 294–303, 2018. DOI:10.1007/978-3-030-05345-1_25.

3. "Using blockchain to improve data management in the public sector," McKinsey & Company, 2017. https://www.mckinsey.com/businessfunctions/mckinsey-digital/our-insights/using-blockchain-to-improvedata-management-in-the-public-sector.

4. "What is Blockchain Technology? - IBM Blockchain," www.ibm.com. https://www.ibm.com/in-en/topics/what-isblockchain.

Sub Problem (Member 02) – Implementing Two-Factor Authentication (2FA) system for the Blockchain based criminal Information Management System.

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. However, like any security measure, 2FA is not foolproof,

- SMS-Based Attacks: SMS-based 2FA is vulnerable to attacks such as SIM swapping, where an attacker takes control of the user's phone number by convincing the carrier to transfer it to a new SIM card.
- Phishing attacks: Attackers can use phishing emails or websites to trick users into revealing their authentication credentials or providing access to their devices.
- Authentication bypass: In some cases, 2FA can be bypassed by exploiting vulnerabilities in the authentication.
- process or in the software or hardware used to generate or store the authentication codes.
- Third-party authentication services: Using a third-party authentication service can introduce additional security risks, as the service provider has access to the user's authentication credentials and can potentially leak them.

References:

1. "What Is SMS 2FA? Text Message Authentication Explained," 20 April 2022. [Online]. Available: https://rublon.com/blog/what-is-sms-2fa/#:~:text=Cons%20of%20SMS%202FA%3A&text=Vulnerable%20to%20SIM%20swapping%20attacks, of%20the%20real%20SIM%20card..

2. P. Markert, F. Farke and M. Dürmuth, "View The Email to Get Hacked:," p. 6, 11 August 2019

3. "Bypass techniques for multi-factor authentication," 23 January 2023. [Online]. Available: https://www.bcs.org/articles-opinion-and-research/bypass-techniques-for-multi-factor-authentication/.

Sub problem (Member 03) – No proper Access control Hierarchy in Sri Lanka criminal information management system

The aim of this research project is to develop a Blockchain based criminal records management system to get rid of paper based criminal records management system due to a lot of real-world problems. According to our research about the criminal records management system in Sri Lanka, there is a traditional way which had been followed by the department of police. This way has various potential problems. I found access control handling as a major problem in the traditional systems. So, I took it as a problem and found out a solution for that. In Sri Lanka, Paper based records has been handling by the officials which has no proper access control hierarchy. Which means anyone in the police department can handle any kind of data in official manner or else unofficial manner. The paper-based evidence, FIR files, complaint files can be destroyed by any staffs due to bribes.

Sub problem (Member 04)

In Sri Lanka, current criminal information management system of criminal evidences has been stored on computers or stored on secondary storage devices like pen drives, hard disks, CDs etc. **In some cases, police departments have centralized criminal information management systems** on their computer systems therefore some following problems are occurring in the existing approach,

- Unauthorized access to the centralized criminal information management system and stealing the criminal records in the physical storage like lockers or cupboard in police departments.
- Criminal information management system relies on accurate and complete data to be effective. If data is entered incorrectly or incomplete, it could result in inaccurate conclusions and decisions that may have severe consequences.
- Lack of Privacy concerns on existing criminal information management system – risk of sharing information that could be used to discriminate against individuals.
- Need to consider on high cost: In the criminal system there will be various type of files are uploaded as criminal evidence therefore need to consider on high storage Database.
- Potential for abuse: If an attacker or any unauthorized persons misuse the system, the data leakage can be happened therefore it can be violated Confidentiality, integrity, availability of criminal records.
- Electronic criminal records are an important aspect of the criminal database management system. Due to the large number of electronic records, there can be high risk. And the most targeted information is to steal criminal personal identification information (PII). [1] [2]

Overall, file management in Criminal information management system is a complex and sensitive task that requires careful consideration of security, accuracy, privacy, and cost concerns.

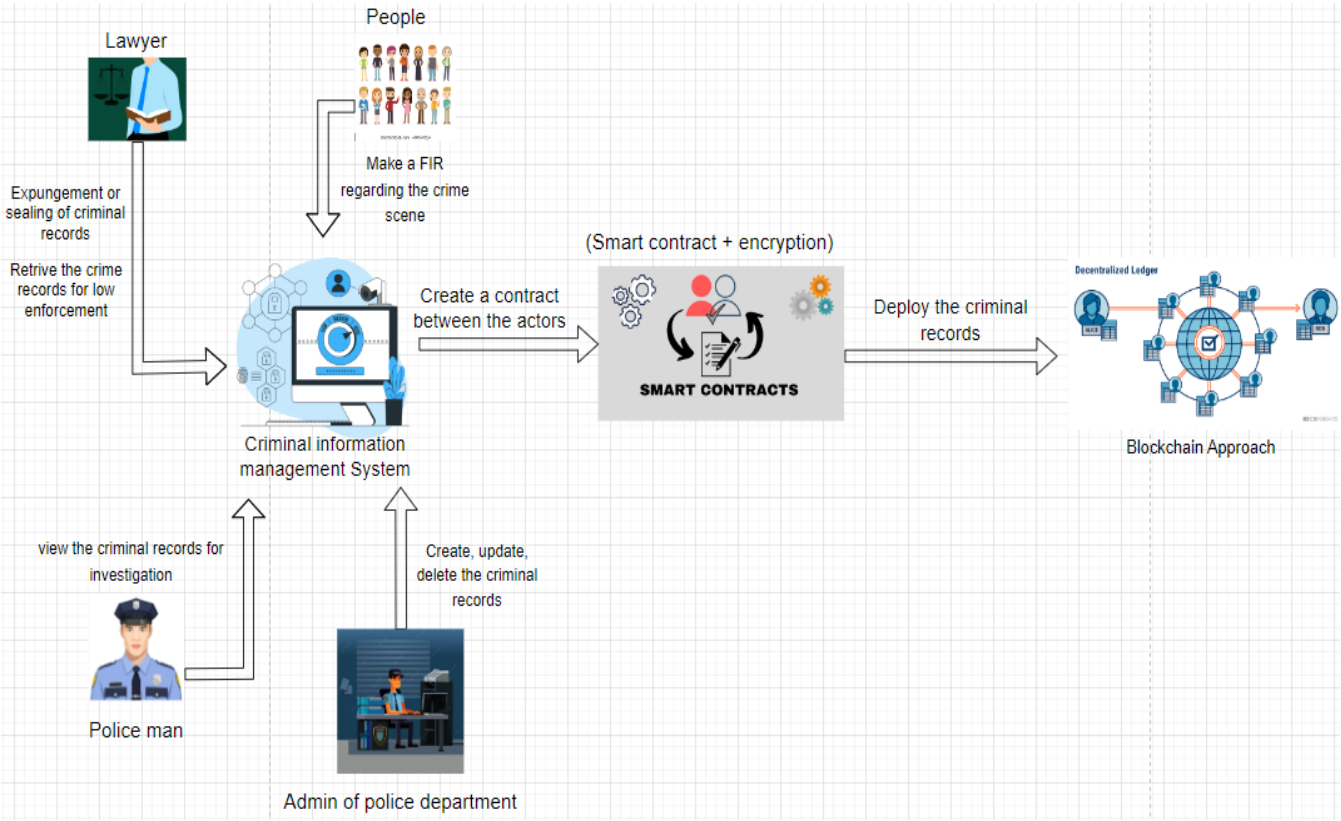
1. S. Routray and R. Ganiga, "Secure Storage of Electronic Medical Records(EMR) on Interplanetary File System(IPFS) Using Cloud Storage and Blockchain Ecosystem," in IEEE Xplore , Erode,India, 2021.
2. A. Jain, S. Das, A. S. Kushwah, T. Rajora and S. Saboo, "Blockchain-Based Criminal Record Database Management," in IEEE Xplore, Pune,India, 2021.

7. Brief description of the nature of the solution (150 words max)

A blockchain based criminal information management system aims to provide a secure and decentralized solution for storing and sharing criminal information. The nature of the solution lies in using blockchain technology to establish a transparent and immutable ledger of criminal records that can be accessed by authorized personnel. The records stored on the blockchain cannot be altered or deleted, providing a tamperproof history of criminal activities. The system can also incorporate smart contract functionality to automate certain processes, such as the notification of relevant parties when a new criminal record is added to the blockchain. This helps to streamline the criminal information management process and reduce the risk of human error. Additionally, the use of blockchain technology ensures the confidentiality and privacy of sensitive criminal information, as the records are stored in a decentralized manner and can only be accessed by authorized personnel through secure authentication methods. In summary, the nature of the solution provided by a blockchain based criminal information management system lies in its ability to securely store and share criminal information, while ensuring transparency, immutability, and privacy.

Solution (Member 01) – Implementing smart contract between criminal information management system and blockchain technology (Blockchain Development)

Developing blockchain technology with smart contract for decentralized criminal information management system for reduce the interoperability of the criminal information management system. Implementing smart contract between the criminal record system and the blockchain approach. The reason of using smart contract in here is smart contract is autonomous, Auto – sufficient, Decentralized. If we deploy the smart contract in our system, we can achieve the following benefits which are secure system, neutrality, immutable can be made due to the absence of hand filled forms in police departments, saves times.

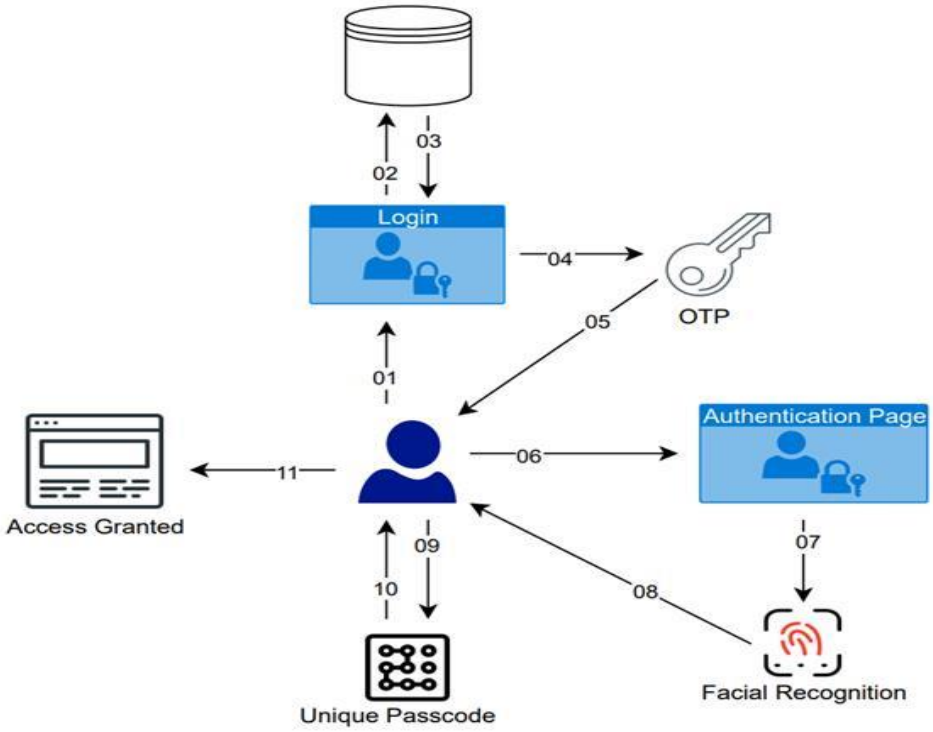


Solution (Member 02) – Implementing Two-Factor Authentication (2FA) system for the Blockchain based Criminal Information Management System.

If we consider 2FA, third-party authentication services will be a solution for SMS-Based attacks. But there are attacks for third-party authentication service providers and you are more vulnerable than being vulnerable to a SMS-Based attack.

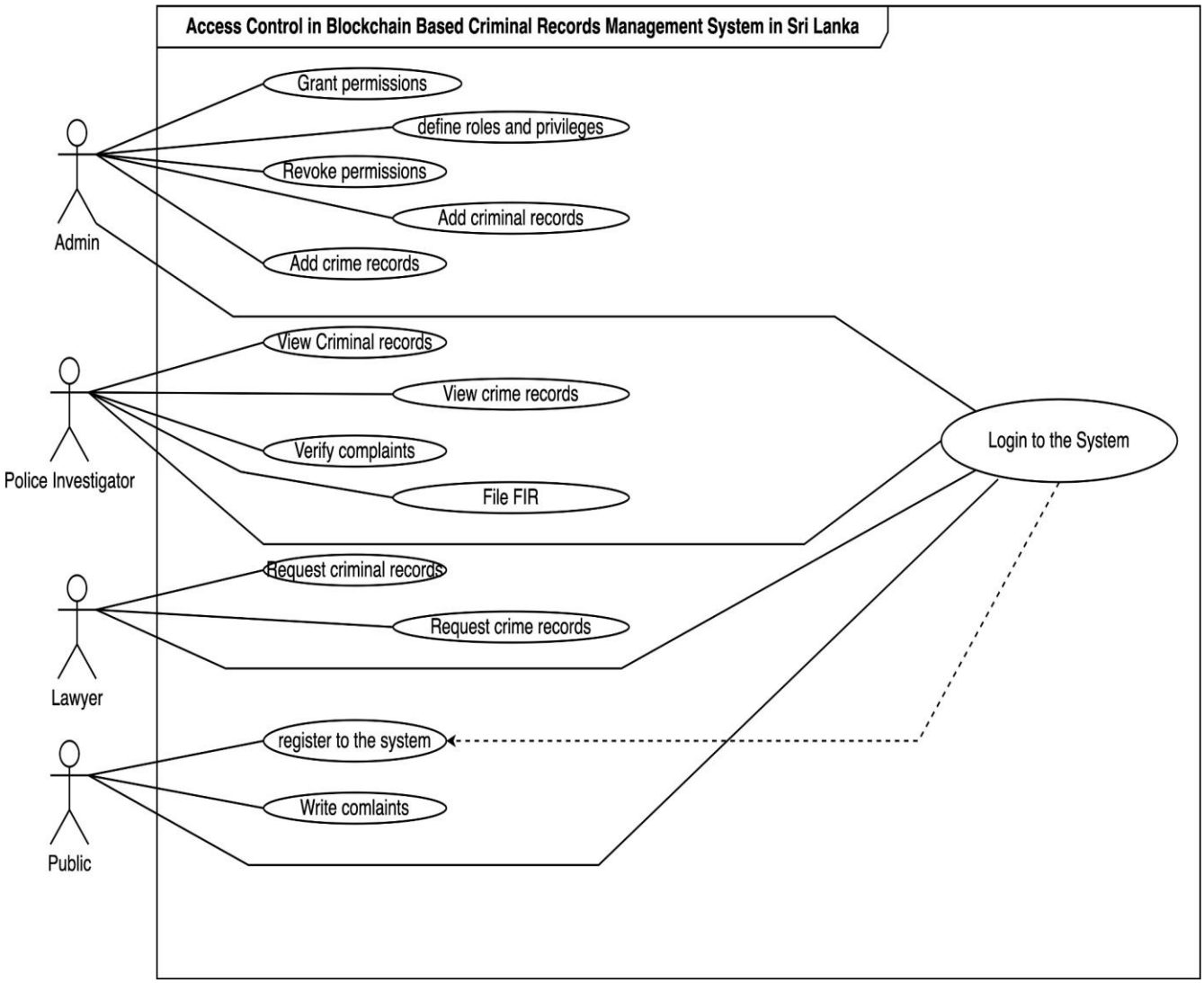
This proposed system, will be using encryption and blockchain to handle the user logins (username and password) as the 1st factor for the authentication and as the 2nd factor it will use a one-time password (OTP) of a length of 6 characters, and this will include digits, letters, and special characters. With the advancement of computation technology, a pin number of 6 digits could be cracked under several seconds with the proper computing power. By implementing an updated algorithm related to Hashed Message Authentication Code (HMAC) and by implementing blockchain I will be improving the security of the OTPs that will be receiving as the 2nd factor. After successfully completing both the 1st and 2nd factor, the user will have to face the 3rd factor, and that will be a facial recognition with a unique, randomly generated passcode that is provided to the user that changes once every 5 days.

With this proposed system, hackers would never access the system by executing phishing attacks and social engineering attacks. Brute forcing the OTP with computers with the capable processing power would still not be enough since there will be the facial recognition system and the randomly generated unique passcode for each user that would change once every 5 days. This proposed system will improve Multi-Factor Authentication for systems with sensitive information such as a Criminal Information Management System.



Solution (Member 03) – Implementing digital access control over the Blockchain based Criminal records management System.

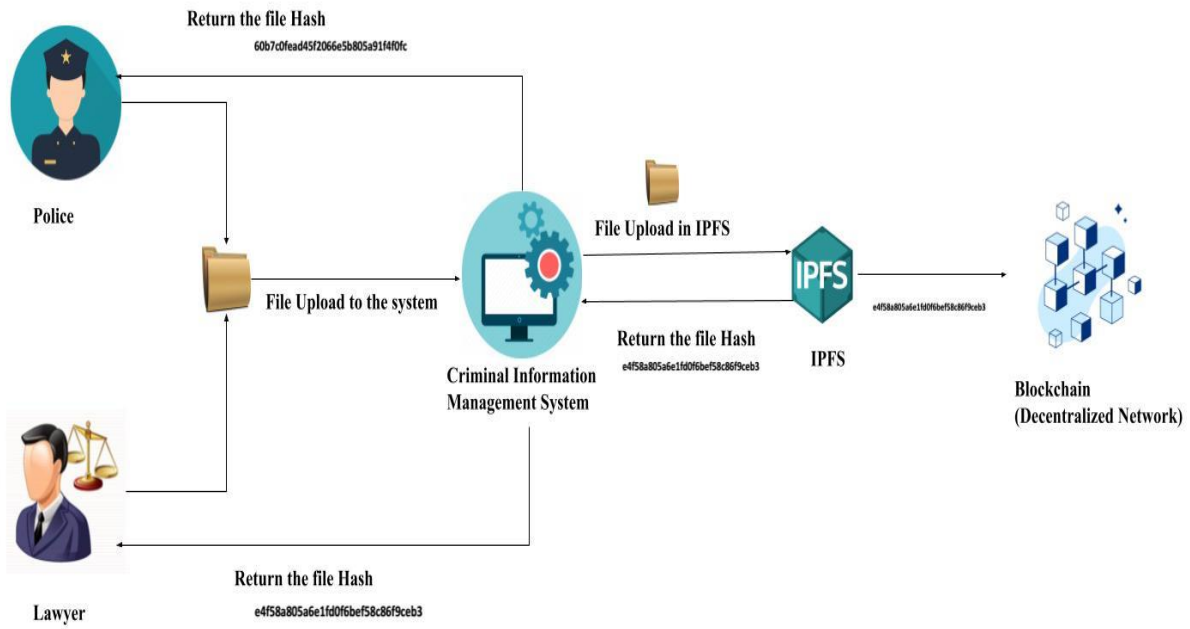
To address this problem, I am going to develop Role Based Privilege Access Control Management System. The permissions are pre-defined according to the roles of the actors. The permissions are based on CRUD. these permissions will be being issued according to their roles by the admin. The admin act as the high privileged actor in the system who handles the entire criminal records database and the other least privileged actors. some can have multiple privileges; some has single privilege which has decided by the admin according to the Sri Lankan of handling the data of a citizen. In Sri Lanka, there is no records that the access control management of the criminal records management system implemented. So, I assume this as my novelty of my research project component.



Solution (member 04) - Implementing secure file management system in decentralized network (Blockchain based Criminal information management system in Sri Lanka)

Developing IPFS for addressed those mention issues. IPFS (Interplanetary File System) is a distributed peer to peer protocol that allows users to store and access files in a decentralized network. IPFS is designed to be a more secure, reliable, and efficient alternative to traditional centralized file storage system. It will minimize the storage issues when storing criminal evidence in criminal information management system. In IPFS, files are broken down into small pieces and distributed across multiple nodes in the network. Each node in the network maintains a copy of the file, which makes it more resilient to failures or attacks. IPFS uses content-addressing to identify files, which means that files are identified by their hash values rather than by their location or path on the network.

Figure 1: Implementing secure file management system in decentralized network.



8. Brief description of specialized domain expertise, knowledge, and data requirements (200 words max)

When developing a Blockchain based criminal information management system, there are required domain expertise, knowledge, and data requirements that will have to be used. The following are a list of the requirements.

- **Knowledge of Blockchain Technology:** Blockchain is being the based for this system, a keen understanding of the execution of blockchain technology, benefits/limitations, and the understanding of how-to applications of this technology are crucial to complete this system.

- **Expertise in Cybersecurity Domain:** Criminal Information Management System, since this system will hold and store sensitive information, implementing cybersecurity to ensure that the system is secure and protected against cyber-attacks is one of the top priorities. This system should be applicable for the CIA tried.

- **Data Management Expertise:** This system will have to handle a large amount of data, and there will be deferent types of users who will be accessing this system, so managing access controls and ensuring all data that are included are accurate, complete, and secure.

- **Knowledge for Algorithm Development:** When monitoring for criminal and suspicious activities that are occurring around the monitored area, algorithms should be developed to identify those activities and separate systems needs to be developed to facial recognition through the receiving feed.

- **IPFS File management system in decentralized Networks:** The Interplanetary File System (IPFS) is a peer-to-peer (p2p) file sharing system that aims to fundamentally change the way information is distributed across and beyond the globe. Although there were some risks while using p2p file sharing technology such as installation of malicious code and exposure of sensitive information, but IPFS enables large-scale and immutable storage by breaking it into small parts and providing timestamps and keeping data secure without having to store the data on the blockchain network. It also creates a permanent and decentralized method of storing and retrieving data by storing a unique hash which is the location of the data.

9. Objectives and Novelty

Main Objective

The main objective of a blockchain based criminal records management system is to provide a secure, transparent, and tamper-proof platform for storing and managing criminal records. The use of blockchain technology can ensure that the records are stored in a decentralized and distributed manner, which makes them more secure and resistant to tampering or unauthorized modification. Additionally, a blockchain based criminal records management system can also help to improve the efficiency of the criminal justice system. By having all criminal records stored in a centralized and easily accessible platform, law enforcement agencies, courts, and other relevant organizations can quickly and easily access the information they need to make informed decisions. This system will also help to identify suspicious or criminal activities in real-time and identify criminals who are in large.

Member Name	Sub Objective	Tasks	Novelty
Brahanawardhan B. IT20150952	**Implementing smart contract between criminal information management system and blockchain technology (Blockchain Development).** • User can securely and effectively store and view the criminal Records. • Ensuring confidentiality, integrity, availability of criminal Records. • Provide a untransparent and secure platform for storing criminals Records. • Decentralized the criminal information management system for increase the accuracy of the criminal records system. • Reducing the interoperability problem when identifying criminal records.	• Define the requirements and information gathering: Define the goals and objectives of the smart contract and the data it needs to manage. • Create a use cases for implementing criminal information management system in blockchain. • Implement overall system diagram for understand the concept. • Choose the right platform: Select the blockchain platform that best meets the needs of the smart contract, such as Ethereum, EOS, or Hyper ledger. • Write the code: Write the smart contract code using a solidity program.	In Sri Lanka, the existing criminal information management system is traditional approach like paper basis. Storing, retrieving, updating the criminal records are highly time consuming. As results, it causes many drawbacks like confidentiality, Integrity, Availability Violation, and scattered data of criminal records. To address the issue our team is proposing blockchain based technology for criminal information management system. To implement this solution, I am going to develop a smart contract between criminal information management system and blockchain approach. According to this novelty concept developing smart contract for criminal records to validate confidentiality, Integrity, Availability, minimize interoperability problem when identifying criminal records and ensure privacy and security of criminal records.

	• To Provide a security, neutrality, no mistake can be made due to the absence of paper basis approach and less time consuming.	• Test the contract: Test the contract to ensure it meets the requirements and functions as expected. • Deploy the contract: Deploy the contract on the blockchain network. • Integrate with Criminal information management system.	
Wijayarathne S.N IT20171438	**Implementing Multi-Factor Authentication system for the Blockchain based Criminal Information Management System** • User login page to enter username and password. • Enhance access control to authenticate and identify the user who is trying to login to the system. • Reduce the risk of identity theft and increase accountability. • Protection against phishing and social engineering attacks. • Comply with regulations depending on the regulations. • Databases to contain the required details to be verified. • Encrypting the stored data with the use of Blockchain.	• Information gathering regarding multi factor authentication and about its functionalities in detail. • Develop an overall system diagram for understand the concept. • Research about facial recognition and one-time passwords. • Selecting the proper cording language. • Create the user interface (UI) for the required login and multi factor authentication. • Cording for the multi factor authentication system. • Developing the database to store login credentials and other required data. • Using encryption and blockchain to increase the security perspective of the collected data.	In the existing 2FA systems or Multi-Factor Authentication system, there are security breachers that could happen and have happed. The users might not always have the required devices with themselves to complete the authentications. This proposed system, will be using encryption and blockchain to handle the user logins (username and password) as the 1st factor for the authentication and as the 2nd factor it will use a one-time password (OTP) of a length of 6 characters, and this will include digits, letters, and special characters. With the advancement of computation technology, a pin number of 6 digits could be cracked under several seconds with the proper computing power. By implementing an updated algorithm related to Hashed Message Authentication Code (HMAC) and by implementing blockchain I will be improving the security of the OTPs that will be receiving as the 2nd factor. After successfully completing both the 1st and 2nd factor, the user will have to face the 3rd factor, and that will be a facial recognition with a unique, randomly generated passcode that is provided to the user that changes once every 5 days.

		• Test the encryption and test the code for the authentication system. • Merge the system with the other parts of the project and test the flow.	
Thushitharan M. IT19983370	**Implementing digital access control over the Blockchain based Criminal records management System.** • Authentication: Verify the identity of users and ensure that only authorized users are granted access to the system. • Authorization: Control what actions and resources each user or group of users can access within the system. • Determine the roles and assign the permissions.	• Identify Access Control Requirements: Determine the requirements for access control in the system, including which actor should have access to which data and permissions. • Develop Access Control Policies: Specify the rules and procedures that govern access to the data. These policies should address issues such as authentication, authorization, and auditing. • Implement Access Control: This is including configuring authentication and authorization rules, determine actors and roles in the police department, setting up user accounts and permissions, and configuring security settings. • Programming: Develop the program using identified programming language. • Test Access Control: Conduct thorough testing of the access control	In Sri Lanka, the existing criminal information management system is traditional approach like paper basis. This has been handling by the officials which has no proper access control hierarchy. Which means anyone in the police department can tamper any kind of data in official manner or else unofficial manner. This is scenario brings huge violation in integrity of the system. To address this problem, I am going to develop Role Based Privilege Access Control Management System. The permissions are pre-defined according to the roles of the actors by the admin. Due to there is no records that the access control management of the criminal records management system implemented in Sri Lanka, I came up with this as my novelty of my research project component.

		mechanisms to ensure that they are working correctly and effectively. • Periodically Review and Update Access Control: Regularly review and update the access control mechanisms to ensure that they remain effective and up to date with any changes to the system or the security environment.	
Ahmed M.N.H IT20157814	**Implementing secure file management system in decentralized network** • The objective is to ensure confidentiality, integrity, and availability of the data. • When police officer or lawyer upload the files into the system. Normally it saves as it is. • When implementing IPFS then it creates new token for each file to identify uniquely. With that token anyone can access the file in the system. • centralized systems are generally easier to control at the same time it is vulnerable to attack. Decentralized technology distributed among the many different entities. So, this technology can be mitigating centralized system vulnerability.	• Design a secure data storage model - Determine the appropriate data structure for storing the files and associated metadata. • Define access control policies to Identify the various roles and permissions for users accessing the system. some users may be authorized to view files, while others may be authorized to add or modify files. • Implement cryptographic techniques Use cryptographic algorithms to secure the data and protect it from unauthorized access. • Integrate with criminal information management system. • Test and audit the system. • Provide a user interface to IPFS.	In Sri Lanka existing criminal information management system need to manage massive amount of criminals' data. To manage the criminal files and records in the current approach in Sri Lanka is not fulfill the requirement it causes some drawbacks such as unauthorized access to criminal records, lack of privacy concerns to minimize this issues I'm going to develop the Secured file system for blockchain based criminal information management system By implement IPFS (Interplanetary File System) for decentralize network. because of my solution it ensure the confidentiality, integrity and availability of the criminal's evidence and data.

10. Supervisor checklist (supervisors should fill sections 10 and 11)

a) Is this research problem valid?

Yes		No	

b) Is the proposed research group, correct?

Yes		No	

c) Is the proposed research area, correct?

Yes		No	

d) Do the proposed sub-objectives match the students' specialization?

Yes		No	

e) Is the required domain expertise, knowledge and the data available?

Yes		No	

f) Is the scope of the solution practical?

Yes		No	

g) Do all sub-objectives have sufficient novelty?

Yes		No	

11. Supervisor details

	Title	First Name	Last Name	Signature
Supervisor				
Co-Supervisor				
External Supervisor				
Summary of external supervisor's (if any) experience and expertise				

Summary Sheet

The topic evaluation panel will use the summary sheet to evaluate the suitability of the project.

1. Brief description of research problem including references (200 – 300 words max)

The increasing number of criminal activities has led to a need for a more efficient and secure system for managing criminal information. According to our analysis, Major problem in our country is maintaining criminal information records in paper basis and one of the key challenges facing the current criminal information management system is the lack of transparency, security, and immutability in the storage and dissemination of information. This has led to numerous data breaches and unauthorized data modification causing significant damage to both individuals, organizations, and government. Blockchain technology has the potential to provide a secure and transparent solution for criminal information management. A blockchain based criminal information management system can use decentralized ledgers to store criminal records, ensuring that the information is secure and tamper-proof. The use of smart contracts can also automate the process of updating and accessing the information, reducing the potential for human error. This system can also provide a secure and transparent platform for sharing criminal information between law enforcement agencies and other relevant. Stakeholders, improving collaboration and coordination in the fight against crime. In conclusion, a blockchain based criminal information management system is a promising solution for improving the efficiency, security, and transparency of criminal information management. This research will contribute to the development of a secure and efficient platform for managing criminal information using Blockchain technology, which can have a significant impact on the criminal justice system and the fight against crime.

2. Brief description of the nature of the solution (150 words max)

A blockchain based criminal information management system aims to provide a secure and decentralized solution for storing and sharing criminal information. The nature of the solution lies in using blockchain technology to establish a transparent and immutable ledger of criminal records that can be accessed by authorized personnel. The records stored on the blockchain cannot be altered or deleted, providing a tamperproof history of criminal activities. The system can also incorporate smart contract functionality to automate certain processes, such as the notification of relevant parties when a new criminal record is added to the blockchain. This helps to streamline the criminal information management process and reduce the risk of human error. Additionally, the use of blockchain technology ensures the confidentiality and privacy of sensitive criminal information, as the records are stored in a decentralized manner and can only be accessed by authorized personnel through secure authentication methods. In summary, the nature of the solution provided by a blockchain based criminal information management system lies in its ability to securely store and share criminal information, while ensuring transparency, immutability, and privacy

3. Objectives and novelty

Main Objective

The main objective of a blockchain based criminal records management system is to provide a secure, transparent, and tamper-proof platform for storing and managing criminal records. The use of blockchain technology can ensure that the records are stored in a decentralized and distributed manner, which makes them more secure and resistant to tampering or unauthorized modification. By having all criminal records stored in a centralized and easily accessible platform, law enforcement agencies, courts, and other relevant organizations can quickly and easily access the information they need to make informed decisions. This system will also help to manage the criminal records and evidence in secure manner and validate confidentiality, integrity and availability.

Member Name	Sub Objective	Tasks	Novelty
Brahanawardhan B. IT20150952	**Implementing smart contract between criminal information management system and blockchain technology (Blockchain Development).**	• Define the requirement and information gathering. • Create a use case for the system. • implement the overall system diagram. • Choose the right platform. • Write the code. • Test the contract. • Deploy the contract. • Integrate with the system.	In Sri Lanka, the existing criminal information management system is traditional approach like paper basis. Storing, retrieving, updating the criminal records are highly time consuming. As results, it causes many drawbacks like confidentiality, Integrity, Availability Violation, and scattered data of criminal records. To address the issue our team is proposing blockchain based technology for criminal information management system. To implement this solution, I am going to develop a smart contract between criminal information management system and blockchain approach. According to this novelty concept developing smart contract for criminal records to validate confidentiality, Integrity, Availability, minimize interoperability problem when identifying criminal records and ensure privacy and security of criminal records.

Wijayarathne S.N IT20171438	**Implementing Multi-Factor Authentication system for the Blockchain based Criminal Information Management System**	• Information gathering regarding multifactor authentication system. • Develop an overall system diagram for understand the concept. • Research about facial recognition and one-time passwords. • Selecting the proper cording language. • Create the user interface (UI) for the required login and multi factor authentication. • Developing the database to store login credentials and other required data. • Testing and implement authentication system. • Integrate with the system.	In the existing 2FA systems or Multi-Factor Authentication system, there are security breachers that could happen and have happed. The users might not always have the required devices with themselves to complete the authentications. This proposed system, will be using encryption and blockchain to handle the user logins (username and password) as the 1st factor for the authentication and as the 2nd factor it will use a one-time password (OTP) of a length of 6 characters, and this will include digits, letters, and special characters. With the advancement of computation technology, a pin number of 6 digits could be cracked under several seconds with the proper computing power. By implementing an updated algorithm related to Hashed Message Authentication Code (HMAC) and by implementing blockchain I will be improving the security of the OTPs that will be receiving as the 2nd factor. After successfully completing both the 1st and 2nd factor, the user will have to face the 3rd factor, and that will be a facial recognition with a unique, randomly generated passcode that is provided to the user that changes once every 5 days.
Thushitharan M. IT19983370	**Implementing digital access control over the Blockchain based Criminal records management System.**	• Identify Access Control Requirements • Develop Access Control Policies • Implement Access Control • Programming • Test Access Control • Periodically Review and Update Access Control • Integrate with the system.	In Sri Lanka, the existing criminal information management system is traditional approach like paper basis. This has been handling by the officials which has no proper access control hierarchy. Which means anyone in the police department can tamper any kind of data in official manner or else unofficial manner. This is scenario brings huge violation in integrity of the system. To address this problem, I am going to develop Role Based Privilege Access Control Management System. The permissions are pre-defined according to the roles of the actors by the admin. Due to there is no records that the access control

			management of the criminal records management system implemented in Sri Lanka, I came up with this as my novelty of my research project component.
Ahmed M.N.H IT20157814	**Implementing secure file management system in decentralized network**	• Design a secure data storage model. • Define access control policies to Identify the various roles. • Implement cryptographic techniques Use cryptographic algorithms. • Integrate with criminal information management system. • Test and audit the system. • Provide a user interface to IPFS.	In Sri Lanka existing criminal information management system need to manage massive amount of criminals' data. To manage the criminal files and records in the current approach in Sri Lanka is not fulfill the requirement it causes some drawbacks such as unauthorized access to criminal records, lack of privacy concerns to minimize this issues I'm going to develop the Secured file system for blockchain based criminal information management system By implement IPFS (Interplanetary File System) for decentralize network. because of my solution it ensures the confidentiality, integrity and availability of the criminal's evidence and data.