International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 10, pp 212-219, October-2023
https://doi.org/10.47001/IRJIET/2023.710028

Blockchain-Based Criminal Information Management System in Sri Lanka

[1]Brahanawardhan B., [2]Wijayarathne S. N., [3]Ahmed M. N. H., [4]Thushitharan M., [5]Ms. Dinithi Pandithage, [6]Mr. Kanishka Yapa

[1,2,3,4,5,6]Department of Computer Systems and Engineering, Sri Lanka Institute of Information Technology (SLIIT), Colombo, Sri Lanka

Authors E-mail: [1]it20150952@my.sliit.lk, [2]it20171438@my.sliit.lk, [3]it20157814@my.sliit.lk, [4]it19983370@my.sliit.lk, [5]dinithi.p@sliit.lk, [6]kanishka.y@sliit.lk

***Abstract* - Due to the current economic crisis in Sri Lanka, people's lifestyles are in difficult conditions. Due to this, crimes are increasing rapidly. The graph of criminal activities is steadily increasing in the country because of an economic crisis and the globalization of ultra-modern technology. In many industries today, blockchain applications are being explored as a secure and cost-effective method to manage a distributed database and keep track of all types of digital transactions. In Sri Lanka, the existing criminal information management system is a traditional paper-basis approach. Storing, retrieving, and updating criminal records are highly time-consuming. As a result, it causes many drawbacks. To address the drawback, our team is proposing blockchain-based technology for a criminal information management system called "CRYSIS." Blockchain can take the position of the accumulation of criminal records with a network where criminal records information is easily accessible within the organization, secure, and cannot be altered. A P2P (peer-to-peer) network called blockchain aids in the decentralization of criminal records. As a result, to maintain a ledger to prevent a single point of failure (SPOF), and all the criminal records will be updated and validated in real-time. Because they are easily accessible and unbreakable, decentralized networks with straightforward algorithms are safe and cryptographically secured. Blockchain's peer-to-peer network facilitates the sharing of information within organizations. To ensure criminal records' confidentiality and integrity, this system will be built on the immutability feature of blockchain. By developing this blockchain-based system, the corruption of risk factors can be reduced.**

Keywords: Blockchain Technology, Criminal Records, Smart Contract, Multi-factor Authentication, Secure File Management, Chain of Custody, Law Enforcement.

I. INTRODUCTION

Criminal information management is a vital component of any effective justice system. Crimes in our daily life are increasing to an uncountable level due to the current economic crisis that Sri Lanka is facing [1]. The daily life of the people in Sri Lanka is in a difficult situation due to allegations of activities like theft, money laundering, bribery, and extortion that are occurring daily due to people becoming criminals and dishonestly within police stations.

Accusations are being covered up as they come due to politics and bribery. One of the main bottlenecks that police stations and departments are facing is the increased number of criminal records and how they can handle them efficiently. As far as Sri Lanka is concerned, the complaint handling and recording of criminal activities are mainly maintained manually and on a centralized system that covers technologically advanced areas.

Due to these limitations and the paper-based method, there are a considerable number of drawbacks and defects that police stations and departments are facing, and some of them are a limited amount of accessibility, lack of transparency, criminal records tampering, records misplacing, and many more. This has made it challenging for law enforcement organizations within Sri Lanka to effectively conduct and proceed with justice for criminals[2].

A potential remedy for these drawbacks is a method based on blockchain technology. Blockchains are distributed, tamper-resistant digital ledgers implemented without a central authority and are tamper-evident. In their most fundamental form, they enable a community of users to record transactions in a shared ledger within that community. As a result, no transaction can be altered after it has been published in the normal operation of the blockchain network [3].Therefore, our team has proposed a "Blockchain-Based Criminal Information Management System" (CRISYS) to address the problem and challenges law enforcement organizations face in Sri Lanka. A blockchain-based criminal information management system

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 212-219, October-2023

https://doi.org/10.47001/IRJIET/2023.710028

could provide improved security and transparency within a decentralized network, aswell as increased efficiency in tracking and handling criminal cases, by utilizing the advantages of blockchain [4].

However, research on the subject is limited, especially in the Sri Lankan context, and the use of blockchain technology in criminal information management is still in its infancy. In the context of the benefits, challenges, and feasibility of a blockchain-based criminal information management system in Sri Lanka, this research aims to investigate its potential.

II. LITERATURE REVIEW

In this section, we review existing literature on blockchain technology, criminal information management systems, and related topics in the context of Sri Lanka's criminal justice system. This section contains previous papers that were reviewed and examined for the purpose of understanding the process, strengths, and weaknesses of the related topics and developing the blockchain-based criminal information management system in Sri Lanka. [4]

Any type of data could be stored in the block. All criminal records will be kept in this block. It contains a unique value called a hash, which, once verified, acts like a fingerprint that is accessible across all network peers; (Fig 1) will display a simplified overview of a data block. Each block contains the following:

- Contains the hash value of the block.
- Cryptographic hash of the previous block.
- The goal of the current difficulty.
- The root hash of Merkle tree.

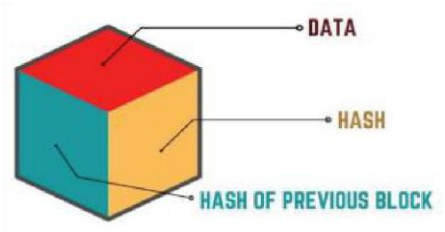

Figure 1: Data Block

It also contains the hash value of the previous block to create a chain of blocks containing the records. As a new record is entered, it creates a new block. Once the block is populated with records, it is merged with the previous block, putting the data together sequentially.

Hash is a mathematical operation that can convert an input of arbitrary length into an encrypted output of a fixed length. As a result, its unique hash value is always the same size, independent of the original data or file size. (Fig 2) will display a simplified overview of the hash in a data block.

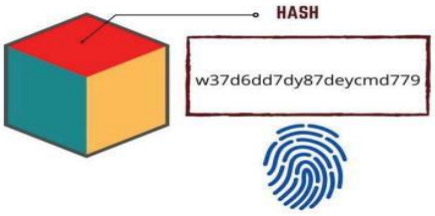

Figure 2: Hash in a data Block

On the other side, hashing is a one-way function that cannot be decrypted back to the original data. A system based on the SHA-256 mathematical algorithm. This methodology will prevent unauthorized access and confidentiality, integrity, and availability violation.[17]

Blockchain and distributed ledger technology are evolving in today's digital world for faster processing and secure transactions. Cryptocurrencies and bitcoin applications use blockchain and distributed ledger technology to perform decentralized transactions.

To overcome this limitation, we propose a methodology to integrate blockchain with IPFS to enhance the throughput and optimize the memory. InterPlanetary File System (IPFS) is integrated with blockchain to enhance the throughput and performance of the application.

In this research paper, to ensure the throughput and performance of the application, they integrate InterPlanetary File System (IPFS) with blockchain. Because of this integration, it performs better in optimizing memory, reducing transaction delay, and reducing transaction processing, and it ensures throughput.

IPFS storage file system that uses Distributed Hash Table (DHT) technology to store and manage massive volumes of data in a decentralized environment.

Blockchain, a revolutionary method of storage and immutability, provides a robust storage strategy and, when coupled with a smart contract, gives users the ability to form partnerships, share information, and consent via a legally based system of carrying out business transactions in a secure digital domain.

This includes isolating packet data to inform levels of cybersecurity and privacy-related activities and ensuring transparency is demonstrated in a secure, smart, and effective manner.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 212-219, October-2023

https://doi.org/10.47001/IRJIET/2023.710028

Further research points out the possible privacy and security advantages of blockchain-based criminal information management systems. It has been proposed as a potential solution to the issue of data breaches and illegal access to private criminal records by Maras and Greenfield (2018) [8]. They proposed a system based on blockchain technology that would provide people more control over their private information while enabling authorized parties to access the data they require for legal reasons.

III. METHODOLOGY

A multifaceted strategy is used in the research plan and architecture to look into developing a blockchain-based criminal information management system. In order to get perspectives on current developments, systems, and optimal procedures connected to criminal information management and blockchain technology, an in-depth body of research will be undertaken first. This will provide a starting point for determining the gaps and difficulties that the suggested solution seeks to address. In order to fully comprehend the needs, demands, and concerns of important stakeholders, including law enforcement organizations, legal professionals, and technological specialists, interviews will also be performed with them. In order to learn about their opinions about the present criminal information management system and what they anticipate from a blockchain-based solution, a survey questionnaire will also be given out to prospective users [9].

To provide insightful conclusions, the data gathered through interviews and surveys will be examined using both qualitative and quantitative techniques. Based on the results, a blockchain-based criminal information management system prototype will be created and put through rigorous testing in a monitored environment. Through exercises and input from users, the system's functionality and usability will be assessed. The findings will be examined, and suggestions for enhancement, scalability, and potential difficulties will be made. A thorough examination of the viability, efficacy, and possible advantages of a blockchain-based criminal information management system in expanding the effectiveness and security of criminal data management operations will be ensured by the approach used.

The use of a number of innovative methods and technologies was required for the creation of a blockchain-based criminal information management system. Ganache, a private blockchain platform that is used in this system to manage criminal records, offers a secure and scalable infrastructure. An agile paradigm was used for the process of developing software, enabling iterative development, constant feedback, and quick adaptability to changing needs.

An IPFS (InterPlanetary File System) system was built to enable safe documents to be stored and retrieved, permitting decentralization and tamper-proof file administration. This technology reduces the potential of data loss or unlawful access while ensuring the consistency and accessibility of criminal records.

The implementation of a multiple-factor authentication mechanism improved system security and authentication. The further degree of security guarantees that only people with the right authorization and authorization can access the system containing sensitive criminal data. The solution reduces the likelihood of inappropriate access and increases overall safety safeguards by utilizing multiple-factor authentication.

IV. BLOCKCHAIN-BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM (EXPECTED CONTRIBUTIONS)

This research is done by a group of four, and each individual will mainly focus on a different research component with gaps. Individually the four components that have been selected can be considered as four pieces of research, with each having its own merits. But, after the completion, there will be a final product with a blockchain-based criminal records management system to provide a secure, transparent, and tamper-proof platform for storing and managing criminal records. The four components were chosen to complete this research project to reach all its merits.

- Implementing smart contracts between criminal information management systems and blockchain technology.
- Implementing a multi-factor authentication system for the blockchain-based criminal information management system.
- Implementing a secure file management system in a decentralized network.
- Implementing chain of custody to the blockchain-based criminal information management system.

The following sections contain the details about the selected four components.

A) Smart Contract for Blockchain

In this part, focusing on the criminal information management system is deployed with the blockchain network. Many challenges limit the accuracy and usefulness of Sri Lanka's traditional paper-based criminal information management system. In Sri Lanka, the current criminal information management system relies on traditional paper-based methods. However, this approach proves to be highly time-consuming when it comes to storing, retrieving, and

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 212-219, October-2023

https://doi.org/10.47001/IRJIET/2023.710028

updating criminal records. Relying only on paper records takes a lot of time and increases the danger of data integrity and confidentiality being compromised. As a result, several issues arise, including violations of confidentiality, integrity, and availability, as well as the scattering of criminal data. To tackle this problem, our team proposes adopting a blockchain-based technology for the criminal information management system. Our solution involves the development of a smart contract in blockchain that establishes a connection between the criminal information management system and the blockchain approach. This innovative concept aims to ensure the validation of confidentiality, integrity, and availability of criminal records. Furthermore, it seeks to minimize interoperability problems encountered when identifying criminal records while prioritizing the privacy and security of such sensitive information [10].

Additionally, the dispersed nature of criminal records makes it more challenging for law enforcement organizations to obtain and correlate information effectively.

We suggest using blockchain-based technology to implement a remedy to these serious flaws. We seek to transform the criminal information management system by utilizing the decentralized characteristics of blockchain and providing greater security, quicker procedures, and accessibility.

This proposed solution, smart contracts, are designed with criminal information management based on the General Data Protection Regulation [GDPR] Act law enforcement policies &procedures. The study synthesis was to evaluate smart contracts' current state in relation to the blockchain-based criminal information management system. The investigation was rigorously carried out by carefully going over the readily accessible pertinent material. The creation of specific research questions, the use of relevant databases, and the application of methodical techniques for the identification and assessment of information were all part of the review process. The goal was to present a thorough and transparent evaluation of the function of smart contracts in the area of blockchain technology to administer criminal information [11].

B) Authentication System

This section aims to understand the implementation of multi-factor authentication in the blockchain-based criminal information management system. The most common multi-factor authentication mechanism starts with the username and password, the 6-digit code, and a security question. The most commonly used base requirement to have a successful password is to have at least eight characters in length with lower and upper case letters [12].

The base of a multi-factor authentication system is a two-factor authentication system with an additional security question. Like any security measure, 2FA needs to be more foolproof. Simplebut effective methods can be taken to bypass two-factor authentication and exploit the required information to exploit two-factor authentication. Mentioned are a few methods of two-factor authentication that can be exploited or bypassed, and they are SIM swapping, social engineering, authentication app compromise, malware, man-in-the-middle attack, and hardware token compromise are just a few examples.

This section proposes a solution to develop a multi-factor authentication system with enhanced security mechanisms within each factor. Since authentication systems are built separately, this system and the method of this system can be used for other applications to enhance their security and protect the users who are using those systems. The following are the enhancements that will be included within this proposed system.

- The first factor – Password length will be enhanced to 12 to 16 characters, increasing the time duration that would take an attacker to break the password. These set passwords will contain numerical, lowercase, uppercase, and special characters; as a special enhancement, the password could not contain segments of the username.
- The second factor – The basic 6-digit code will be enhanced to a 6-character code. This will increase the number of possibilities from 59,049 to 60,466,176 possibilities.
- The third factor – A simple but elegant facial recognition inherent factor will be introduced with an additional security layer; a security pin code that will be unique to each user for a time duration.

C) Secure File Management System

When thinking about criminal information management systems, the system needs to handle a massive amount of data such as forensic data, criminal records, evidence, and FIR records. [13] It can be a document, image, audio file, video file, etc., in the currently existing system in Sri Lanka. It is a traditional paper-based management system and a centralized database management system. It can lead to DoS attacks, SQL injections, XSS attacks, internal and external attacks, unauthorized data modification theft, etc. [5] It violates the integrity, confidentiality, and availability of the data. Criminal personal identification information. To address this challenge, implementing a secure file management system in a decentralized network. In a blockchain, there are some limitations to storing large files and documents. It can only store lightweight textual information inside the block to store

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 212-219, October-2023

https://doi.org/10.47001/IRJIET/2023.710028

heavyweight information, IPFS is utilized. It is a peer-to-peer protocol. Each file generates a unique hash value for the store file according to the content of the file. [14] [15] IPFS content address increases the integrity of the transaction by owning to the hash. [16] The system ensures that criminal information is stored in a tamper-proof and transparent manner, which reduces the risk of unauthorized access, data breach, and information modification. And only can be accessed by authorized personnel through secure authentication methods. [17] The file can be uploaded into a secure file management system in two methods. To store files and documents permanently and to share files between two parties.

1) To Store Permanent Files and Documents

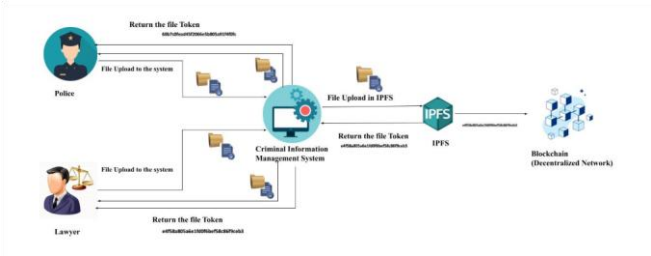

Figure 3: Secure File Management in Decentralized System

(Fig 3) To store permanent files and documents in IPFS, implement symmetric encryption to encrypt the file. And storing keys in a secure way. When a user needs to access the document where it is required to decrypt the file before access

2) To Share Files Between Two Parties

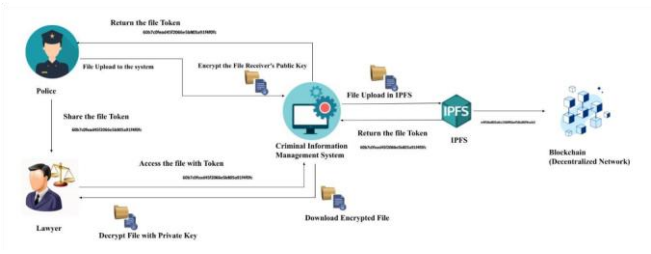

Figure 4: Secure File Sharing in Decentralized System

(Fig 4) When sharing the file between two parties, the sender encrypts the file with the receiver's public key and shares files through the IPFS when receiver accesses the file, it is necessary to decrypt the file with receiver's private key to access the file.

The encrypted files are stored in IPFS.It generates a unique hash value(token) for each file and retrieves the hash value. At the same time, the token will be sent to a decentralized network. The file can be accessed by anyone through the decentralized network. But files and documents cannot read or see the valid content without decrypting the file.

D) Blockchain Chain of Custody

This component focuses on the implementation of a blockchain-based chain of custody in the proposed system, which aims to establish a secure and transparent framework for tracking the movement and managing the logs of digital evidence. The traditional chain of custody process is handled paper-based, and it has major problems such as lack of transparency, data tampering, and lack of evidence log management. This leads to the difficulty in verifying the integrity of records. By leveraging the distributed and immutable nature of blockchain technology, this system will rectify these problems in the existing system.

The blockchain chain of custody system comprises the Evidence DB, Evidence Log, and Frontend Interface. The Evidence DB stores the actual digital evidence, while information about the Chain of Custody is stored in the Evidence Log, which utilizes blockchain technology. This division is necessary due to the size limitations of the blockchain and the need to restrict access to authorized nodes. Only information about the CoC process and a hash of the evidence are stored in the blockchain, ensuring verification while maintaining security.[18]

- Evidence DB– The original digital evidence is stored in the Evidence DB along with a unique ID generated from the evidence's hash and a nonce. This database is managed by trusted organizations, such as law enforcement personnel in courts. Access to the evidence is granted only to authorized organizations based on their respective roles and permissions.
- Evidence Log– The Evidence Log utilizes blockchain technology to store details about each piece of evidence, such as its ID, description, submitter's identity, and the complete history of ownership. While the evidence is not directly stored in the blockchain, the ID generated using a secure cryptographic hash function ensures the integrity of the evidence. The evidence log is built on a peer-to-peer network consisting of authorized entities.

This component brings various advantages to the Department of Police Sri Lanka compared to the existing paper-based system. They can ensure the integrity of digital evidence and ensure the process by the log management of the evidence. This system can find applications in various industries, including supply chain management, legal proceedings, and the handling of valuable assets, ultimately promoting efficiency, trust, and accountability. But the ultimate goal is to implement this proposed system for the Department of Police Sri Lanka.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 212-219, October-2023

https://doi.org/10.47001/IRJIET/2023.710028

V. ANTICIPATED RESULTS AND ANALYSIS

Through this proposed mechanism and system, we expect to help law enforcement in Sri Lanka to build a better country for citizens with fewer crimes and a better system to monitor stored criminal records and record new criminal activities.

With the implementation of blockchain in the criminal information management system within Sri Lanka, all data and records will be stored in a decentralized network and system and will contain a tamper-proof mechanism. We anticipate that this proposed system will provide more security for police stations and police departments and help them with time management by making the entire process shift from a document-based (paper-based) approach to an online system-based approach. The blockchain implementation will provide the required security for the inserted records and evidence.

To enhance the security when a user logs into the page is anticipated to be enhanced with the newly proposed multi-factor authentication mechanism. With the enhanced password length and the shift from a 6-digit code to a 6-character code, the time needed to break such a code will increase, and the possible combinations would increase nearly 1024 times compared to a 6-digit code. This will make it more secure for the end users and the system owners to keep their required systems and data safe. Additionally, since the multi-factor authentication system is built separately, this could be used with any other system or software, and it will be compatible.

When it comes to criminal records, files play a major role. So, as well as keeping the data inserted into the system securely, it is our responsibility to provide security to the files that can contain the records, such as audio files, investigation video files, snapshots, etc. By using an InterPlanetary File System (IPFS), we are anticipating toprovide the required security. As an additional layer, the required files will be encrypted prior to the upload to the IPFS system and stored with the base of the blockchain. When recovering the stored files, the required parties will need to have the decryption keys to decrypt the file encryption and do the needful.

VI. DISCUSSION

The studies discussion part establishes links connecting what was discovered and the subject of the study question while offering an interpretation and analysis of the expected results. The purpose is to clarify any potential repercussions of the projected outcomes for the creation and deployment of the blockchain-based criminal information management system. The deployment of a blockchain-based system has the potential to considerably improve the effectiveness, security, and transparency of criminal information management when the expected outcomes are analyzed. Because blockchain technology is decentralized, it is impossible to tamper with the data that is stored there, protecting the accuracy and dependability of criminal records. Additionally, the usage of smart contracts makes procedure automation possible, speeding up database administration and lowering manual mistakes.

By making it possible for key parties, such as law enforcement authorities, the judiciary, and government bodies, to collaborate and share information in an efficient manner, the projected results have the ability to completely transform the criminal justice system. Criminal records' improved openness and mobility can help identify persistent felons quickly, enhancing the efficiency of inquiries and the administration of justice as a whole.

Due to legal and moral constraints, it is expected that accessing pertinent criminal records throughout the entire study process may prove difficult. It will be essential to work together with law enforcement authorities and other interested parties to overcome these obstacles and guarantee the availability of accurate and comprehensive information for analysis.

The results of this study should show that maintaining criminal records has grown more efficient, secure, and transparent. But while upholding ethical and legal obligations, it is crucial to address issues with scalability, interoperability, privacy, and data protection. By overcoming these obstacles, a strong blockchain-based system that has a revolutionary influence on the management of criminal information and makes a substantial contribution to the administration of justice can be created.

VII. CONCLUSION

A significant milestone in the area of criminal justice is the installation of a blockchain-based criminal information management system. Through the use of the private blockchain Ganache, an agile software development life cycle, IPFS for secure file management, multifactor authentication, and a chain of custody procedure, this research study has examined the potential of blockchain technology. The system addresses the shortcomings of conventional paper-based systems by utilizing these methods and technologies to secure the confidentiality, integrity, availability, and accountability of criminal information. The blockchain-based approach to criminal record storage, retrieval, updating, and authentication offers enhanced confidentiality, transparency, and efficiency. Additionally, it increases the overall operational performance of the criminal justice system, streamlines information management procedures, and makes criminal evidence more credible. With regard to issues including scalability, interoperability, and compliance with laws and regulations, it

ISSN (online): 2581-3048
Volume 7, Issue 10, pp 212-219, October-2023
https://doi.org/10.47001/IRJIET/2023.710028

is crucial to admit that more investigation and creation are required. Overall, the widespread utilization of a blockchain-based system for managing criminal convictions has enormous potential for transforming the way criminal paperwork is handled and paving the way for a future criminal information management system that is safer and more effective.

ACKNOWLEDGMENT

We would like to take this opportunity to publicly express our gratitude to our mentors, Supervisor - Mr. Kanishka Yapa and Co-Supervisor - Ms. Dinithi Pandithage, as well as the entire research project team. We would like to express our sincere gratitude to everyone who contributed to this study. We would like to begin by expressing our appreciation to our supervisors for their guidance and support throughout the study process.

Additionally, we would like to express our gratitude to all our friends and family members for showing us all the support and advice provided for us to work on this research paper. With their input and suggestions, we were able to look into various different paths and continue with this research.

REFERENCES

[1] W. Athukorala, "Pera study proves link between economic crisis and rising crime rate," 08 January 2023. [Online]. Available: https://www.sundaytimes.lk/230108/news/pera-study-proves-link-between-economic-crisis-and-rising-crime-rate-507749.html. [Accessed 19 June 2023].

[2] "A predictive State? Sri Lankan context of predictive policing," 25 January 2021. [Online]. Available: https://www.ft.lk/columns/A-predictive-State--Sri-Lank an-context-of-predictive-policing/4-712051. [Accessed 19 June 2023].

[3] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," Cornell University [arXiv], Ithaca, United States, 26 June 2019.

[4] J. Strebko and A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology," in 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), November 2018.

[5] A.Jain, S. Das, A. S. Kushwah, T. Rajora and S. Saboo, "Blockchain-Based Criminal Record Database Management," in 2021 Asian Conference on Innovation in Technology (ASIANCON), August 2021.

[6] M. 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," Procedia Computer Science, vol. 215, pp. Pages 370-379, 2022.

[7] V. Wylde, N. Rawindaran, J.Lawrence, R.Balasubramanian, E. Prakash, A. Jayal, I. Khan, C. Hewage and J. Platts, "Cybersecurity, Data Privacy and Blockchain: A Review," Cyber Security and Privacy in Communication Networks, vol. 03, 12 January 2022.

[8] M. H. Maras and V. A. Greenfield, "Blockchain technology: Implications for data privacy and security in criminal justice," Journal of Criminal Justice Education, vol. 03, no. 29, pp. Pages 369-382, 2018.

[9] 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.

[10] A.Abuhashim and C. C. Tan, "Smart Contract Designs on Blockchain Applications," 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 2020, pp. 1-4, doi:10.1109/ISCC50000.2020.9219622.

[11] V. Aleksieva, H. Valchanov and A. Huliyan, "Smart Contracts based on Private and Public Blockchains for the Purpose of Insurance Services," 2020 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2020, pp. 1-4, doi:10.1109/ICAI50593.2020.9311371.

[12] "Password Strength in Auth0 Database Connections," auth0 by, [Online]. Available: https://auth0.com/docs/authenticate/database-connections/password-strength. [Accessed 19 June 2023].

[13] E. Onuiri, A. Oludele, O. O. A and S. O. O, "A REAL-TIME CRIME RECORDS MANAGEMENT SYSTEM FOR NATIONAL SECURITY AGENCIES," 2015.

[14] S. Reno, S. Bhowmik and M. Ahmed, "Utilizing IPFS and Private Blockchain to Secure Forensic Information," in 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), Rajshahi, Bangladesh, 2021.

[15] H.-S. Huang, T.-S. Chang and J.-Y. Wu, "A Secure File Sharing System Based on IPFS and Blockchain," in Proceedings of the 2020 2nd International Electronics Communication Conference, 2022.

[16] R. Kumar and R. Tripathi, "Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain," in 2019 Fifth International Conference on Image Information Processing (ICIIP), Shimla, India , 2020.

[17] Scalable Blockchain Architecture using off-chain IPFS for Marks Card Validation done by M. Dhulavvagol Praveen, S G Totad, Mahadev Rashinkar, Ribhav Ostwal, Suprita Patil, and Priyanka M Hadapad on ‘Procedia Computer Science: Volume 215, 2022 [6].

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 212-219, October-2023

https://doi.org/10.47001/IRJIET/2023.710028

AUTHORS BIOGRAPHY

Brahanawardhan B.,
Undergraduate, Department of Computer Systems and Engineering, Sri Lanka Institute of Information Technology (SLIIT), Colombo, Sri Lanka.

Wijayarathne S. N.,
Undergraduate, Department of Computer Systems and Engineering, Sri Lanka Institute of Information Technology (SLIIT), Colombo, Sri Lanka.

Ahmed M. N. H.,
Undergraduate, Department of Computer Systems and Engineering, Sri Lanka Institute of Information Technology (SLIIT), Colombo, Sri Lanka.

Thushitharan M.,
Undergraduate, Department of Computer Systems and Engineering, Sri Lanka Institute of Information Technology (SLIIT), Colombo, Sri Lanka.

Citation of this Article:

Brahanawardhan B., Wijayarathne S. N., Ahmed M. N. H., Thushitharan M., Ms. Dinithi Pandithage, Mr. Kanishka Yapa, "Blockchain-Based Criminal Information Management System in Sri Lanka" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 10, pp 212-219, October 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.710028

****

