Evidence Collection Reporting using Blockchain for Preserving Integrity of Digital Investigation

[1]Hari M, https://orcid.org/0009-0002-6538-1759
[2]Jubilant J Kizhakkethottam, https://orcid.org/0000-0001-5512-0067
[2]Tibin Thomas, https://orcid.org/0009-0005-9143-8546
[2]Arun Madhu, https://orcid.org/0000-0001-6181-5420
[1]*Research Scholar, APJ Abdul Kalam Technological University, Kerala, India*
[1,2]*Computer Science and Engineering Department, Saintgits College of Engineering, Kottayam, Kerala, India*

Corresponding Author: *Hari M (email: hari.m@saintgits.org)

***Abstract* - In the current scenario, crime rates increase day by day. The police department plays a vital role in maintaining law and order, and to enforce safety. The project is aimed to develop a blockchain based record keeping system for crime investigation details using smart contract. This can be used to report various crime activities with much authenticity than the traditional way of maintaining records. The records are stored in the database using blockchain architecture and validation is done using proof of work. This is implemented as an online web application using python framework in which police officers can store crime details and FIR details and is managed in a distributed environment. The project interface is made user friendly so that the officials can use it without much learning. The FIR is maintained around the block chain concept in which blockchain administrators play the role of decision makers. Each block is created using finger printing and implemented using the SHA-256 algorithm.**

Index Terms - blockchain, crime record management system, chain of custody, first information report, hashing.

I. INTRODUCTION

More than a million documents are shared over the internet every single hour. In this superfast world, there is a need for ways to share documents easily and securely over the web. There is also a chance for these documents to be tampered upon, making the process always at risk. To resolve these issues, a document sharing system based on blockchain technology and smart contracts that ensures sharing of documents with authenticity and reliability of a tamper proof system is proposed.

Criminal records are highly sensitive public documents, and ensuring their authenticity and protection is crucial. By incorporating police station case records into a blockchain, the integrity and security of these records can be maintained. Blockchain technology decentralizes data using a peer-to-peer network, preventing unauthorized changes and safeguarding the information from adversaries. This decentralized storage system not only protects data but also allows law enforcement officers to efficiently manage criminal records and case information. Moreover, selected organizations or individuals, such as airports and visa application centers, can access these records for relevant purposes, ensuring timely case enforcement and rulings.

Blockchain technology also plays a critical role in maintaining the confidentiality and integrity of First Information Reports (FIR), a key document required to initiate any criminal investigation. After the FIR is registered, the next step is to gather evidence, which must be presented in court. For this process to be effective, the FIR must remain tamper-proof and confidential. A blockchain-based record management system ensures the safety of these records, as only authorized users can access and modify the data, preventing external interference or corruption.

By implementing blockchain in criminal records management, the system enhances transparency and accountability within law enforcement. It eliminates the possibility of data tampering, which can often be a consequence of corruption. This secure framework not only protects case records but also ensures that judgments are delivered in a timely manner, reducing delays and increasing trust in the legal system (Tasnim et al., 2018).

The system uses SHA256 hashing algorithm to generate hash keys and thus implementing fingerprinting using it. Each node in a blockchain ledger will be a valid transaction and group of nodes combined together to form a block. Once a block is generated, it cannot be edited or malfunctioned. Each block is linked to the next block through hashing function, thus preventing intruders from tampering in.

The aim of this paper is to implement the digital crime record management system using blockchain technology to make it more secure and tamper proof. In this era of computers, all distributed systems depend of digital data and thus, securing such systems is of greater importance.

The objectives of the system are to record every crime reported, register the corresponding FIRs, make them visible to authorized users, maintain blockchain log and ledger, store information using encryption and retrieve information using decryption.

II. RELATED WORK

A. *Theoretical Investigations*

A literature review is an essential foundation for research, offering a detailed exploration of recent studies and trends within a specific subject area. For this project, the focus is on crime record management systems and blockchain technology, both of which have undergone significant advancements in recent years. By examining various published articles, this literature review highlights how these technologies intersect and how blockchain can enhance trust and integrity in digital forensic investigations.

Crime Records Management Systems (CRMS) play a pivotal role in crime prevention, identification, and prosecution. However, they are often based on vulnerable frameworks for data management. According to Pandian et al. (2020), police efficiency and reliability in addressing crime are directly influenced by the quality and accessibility of data within these systems. CRMS frameworks aim to integrate data across cities and states, allowing law enforcement to access unified databases efficiently. This distributed architecture and centralized data depot concept enable more efficient and effective investigations.

Oludele et al. (2015) further explored the significance of CRMS in a study focused on real-time crime records management systems for national security agencies. They emphasized how automated CRMS have been adopted globally to track crime and criminal records. Crime, being a societal menace, requires vigilant monitoring to ensure public safety. Therefore, CRMS provide law enforcement agencies with a reliable tool for maintaining records and enhancing their operations' efficiency.

One challenge CRMS face is the lack of comprehensive information that can aid in solving and preventing crimes. According to Svedha (2020), existing communication mechanisms between citizens and law enforcement often fall short, as detectives are unable to gather enough details from victims and witnesses. A new system focusing on crime knowledge mining through natural language processing is proposed. This system would extract critical details from police reports, media articles, and victim or witness accounts, providing a more robust dataset for investigations.

As blockchain technology emerges as a promising tool to address data integrity issues, it is crucial to consider its role in combating mistrust and disinformation. The study "Searching for Trust" delves into the growing concerns surrounding trust in institutional and epistemological systems (Chelsea et al., 2021). This paper highlights how the shift from traditional record-keeping practices to computational information processing threatens the integrity of records, contributing to disinformation and diminishing trustworthiness. Blockchain, with its emphasis on immutable and tamper-proof records, offers a potential solution to these concerns.

In "Multidisciplinary Blockchain Research and Design," Chelsea et al. (2021) examine how theoretical blockchain models can enhance collaboration and learning. Through a three-layer trust model, the study outlines how blockchain can facilitate interdisciplinary communication and design solutions. This model is particularly relevant to the field of digital forensics, where establishing trust in data handling and evidence integrity is paramount.

Blockchain's potential benefits extend beyond trust to areas such as collaboration, organization, identification, credibility, and transparency, as explored in "A Review on Blockchain Technology and Blockchain Projects Fostering Open Science." The paper underscores how blockchain's unique characteristics make it an attractive technology across industries seeking to enhance trust and transparency.

Although blockchain is still in its early stages, as noted in Xu et al.'s (2019) systematic review, its disruptive potential cannot be ignored. While the current body of blockchain research is still developing, the technology has already demonstrated significant promise in transforming industries, including digital forensics and crime record management.

Finally, Levis et al. (2021) discuss the future of blockchain technology, which has generated considerable excitement and speculation about its transformative capabilities. This innovation, particularly its potential to create immutable records, could revolutionize how digital forensic evidence is stored, managed, and authenticated.

In summary, the convergence of CRMS and blockchain technology presents an opportunity to enhance the integrity, security, and transparency of crime-related data. This literature review underscores the necessity of further research into integrating blockchain within CRMS to ensure trustworthy, tamper-proof records, thereby improving the overall efficacy of digital forensic investigations.

B. Modelling

Crime record management system is essential for maintaining law and order and to ensure safety of citizens. People of criminal background can be identified, and they can be made watchful. Such records can be used for case studies and references. But, the high confidentiality and integrity of such records make it difficult to store and keep safe. Several mechanisms like encryption, centralization is used, but still lacks or assures 100% safety. Tampering such crime records can cause severe threats to the society.

The existing system is a web application where a user can login from anywhere in the world. This makes the system more vulnerable. Cybercrimes have different punishments in different countries. The law is different everywhere, so it's easy to intrude to such systems from a country where legal punishment is less. Similarly, an intruder can easily spot vulnerability points in the system as web application has less security compared with console ones.

The system connects different police stations by independent user credentials. Thus, when an employee wants to do phishing or identity theft, he can easily do. Even a single user of the system can manipulate the records without much effort. User credentials can be easily hijacked, and data can be retrieved, deleted or manipulated. This can cause serious harm to the public. There is no proof of work as who did what, when and, how. This makes the system vulnerable, and it affects the integrity of the system.

It is evident that existing crime record management system uses traditional databases to store records. After reviewing the characteristics and properties of block chain, it is clear that the current record management system can be merged with blockchain technology for security and safety. Such an integrated system using smart contract can overcome all disadvantages incurring with existing record management system. Since FIR kind of records are highly confidential and should be kept tamper proof, it is obvious that the concept of blockchain can be efficiently make the system reliable.

III. System Analysis

A. *Proposed System*

The disadvantages of the existing crime record management system make it difficult to implement in real world scenario. Such implementation may incur several monetary expenses for providing safety and security. Much of the time is unwantedly spent on ensuring security features rather that improving system performance and expansion. This makes the system less productive and reduces the scope of improvement. Many advances safety features can be incorporated with existing system. But that requires additional installations, purchase, training and expenses. Thus, a more sophisticated and effective system for ensuring security and safety should be introduced in order to make the crime record management system more effective and freer from tampering.

Introducing the concept of blockchain reduces all the efforts and concerns regarding security management for confidential systems. This concept can be applicable to any industry, any system where confidentiality is a factor. The system ensures proof of work so that no one from outside or inside can be able to tamper the system. The entire system is built under the concept of distributed architecture in which same data is shared among every person who is authenticated to view it. A change in those data can't be made by an individual person as the change only reflects in his copy, all other remains the same, thus, considering it as an invalid transaction.

B. *System Architecture*

In proposed system, 4 types of user access are provided. The superuser in this project is the admin who determines the blockchain Admins and authenticates police officers and users. Upon successful login, User can access the User Database to add records or view data. Similarly, upon successful login with credentials, Police Staff or Station can access the Crime Record Database to accept/reject records added by users, add evidence, and add FIRs. There are 3 authorized Blockchain Admins who have the superpower to approve or reject records. Upon accepting records, a block is created, and they are able to access the blockchain ledger to view transactions.

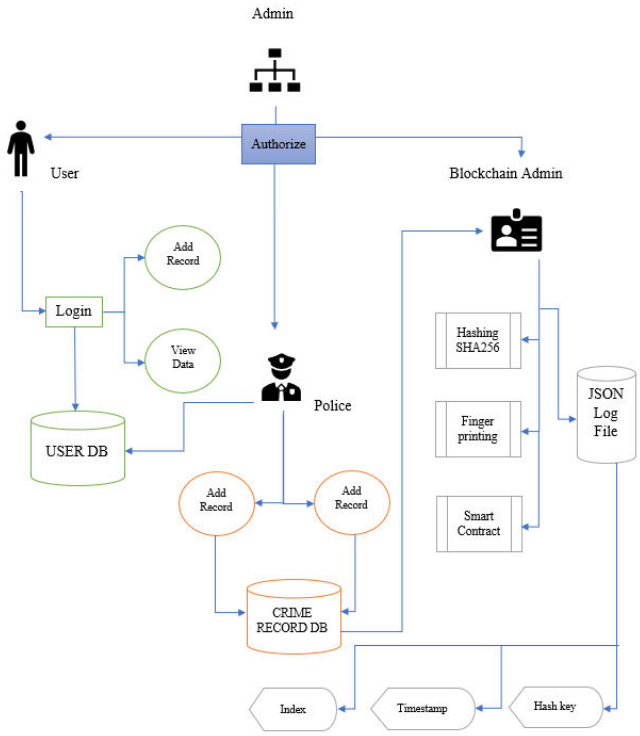

Fig. 1 Architecture

C. *Benefits of Proposed System*

This proposed system has high potential to bring in many benefits to forensic applications by maintaining integrity, transparency, authenticity, security, and auditability of digital evidence to achieve the desired end. Some of these benefits are summarized below.

- Blockchain can strengthen evidence collection, preservation, and validation.
- Provenance for an event or action can be traced back to where it first entered the process under scrutiny.
- Enhances the productivity of executing a transaction with cost savings in specific types of transactions as increased transparency eliminates the need for a trusted third party only to validate some of the claims or only to transfer proof and increases the confidence of the communicating parties.
- The fraud is minimized due to increased transparency of the audit trail.
- Verification at an event or action by organizations can be added at the point of embedding into evidence.
- The record itself is, therefore, a well-set and continuing evidence, to be made available and verifiable.

IV. Design & Implementation

A. *System Design*

The proposed system is built around the concept of block chin architecture where security is of greater importance. It has been used by police department to maintain crime records

which are highly confidential and should be kept tamper proof. The system is developed using Python and Django framework and using the IDE Pycharm. The different modules in the system are identified as follows:

Data Storage: This module deals with data entry and data storage. The complaint registration happens here. After registering the complaint, a detail FIR is framed and stored in the database. Once it is stored, then it can't be edited. The entered FIR will be verified by all the blockchain administrators in the Private Blockchain Network. After that it is going to the blockchain ledger.

Data Encryption: Every blockchain administrator will have his private key for logging purpose. With the private key, a mathematical hashing function is executed, and a hash key is generated. The blockchain ledger will be viewed in encrypted mode. This is done for security purpose. It prevents unauthorized access to the FIR information. When a user login to the system, the system checks if he is a blockchain administrator. If so, it prompts for the private key of the user and checks if it is valid. Then if he tries to access the blockchain ledger, the hash key is generated using his private key and compared with the credential and confirms his account. If he is not a valid user, the encrypted view is visible and if the hash key matches, then the ledger is decrypted and made visible.

Data Retrieval: Data stored in encrypted form can be decrypted while retrieving by providing correct user credentials. Two types of data are maintained. One is the usual crime record information which is been stored in the database. Other is the blockchain information which is stored as JSON format. JSON format is easy to implement and read.

Transaction Validation: This module is the backbone of the whole system. It deals with complete blockchain management which uses encryption, hashing, validation using proof of work and smart contract implementation. The data in the blockchain is stored in blocks and each block contains different types of data. To differentiate between these multiple blocks, fingerprinting is used, and to generate fingerprints, SHA256 hashing algorithm is used. Each block of data includes its own hash and the hash of its previous block. So, this prevents the block from being tampered. After generating a new block, it gets added to the chain. After each addition, the validation of the block is also done.

B. Data Flow Diagram

Understanding the connections between the various system components is made easier with the aid of an analysis model. The analysis model clearly demonstrates to the user how the system will operate. This is a system's first technical depiction.

1) Level 0

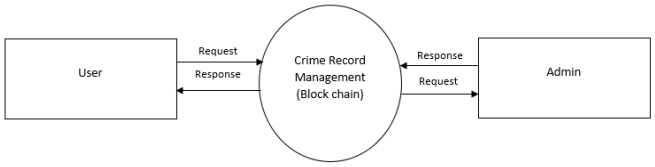

Fig. 2 Level 0 Data Flow Diagram

The basic data flow is that users access the system to send requests to upload records through a digital device to the server and receive responses. Each time, the admin approves or rejects records, a transaction is initiated in the blockchain to ensure security.

2) Level 1

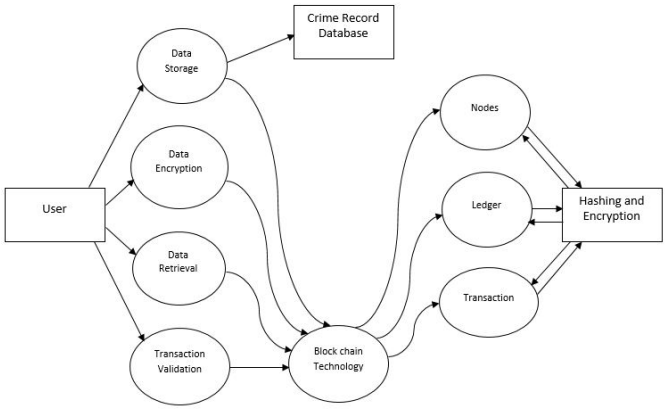

Fig. 3 Level 1 Data Flow Diagram

In Level 1, the data flows in such a way that users based on their roles (user, police and blockchain admin) can perform all or specific functions – data storage, encryption, retrieval and validation of transactions. Blockchain admins can perform all functions while officers perform all functions related to data. Users on the other hand can only access the storage and retrieval of data. All data is stored in the crime record database. The system functions with blockchain technology which includes nodes, ledger and transactions which are all encrypted using the SHA256 Hashing Algorithm.

C. Entity Relationship Diagram

The E-R diagram represents the structure of the database of the system. It is like the blueprint of the database that can be used at a later stage of implementation. The entities and relationship sets are the primary components of the E-R diagram. An entity set is a collection of similar entities, and the entities within such sets can have attributes. The diagram establishes the relationship among those entity sets. The ER diagram is the complete logical structure of a database, such that it demonstrates relationships among tables and their attributes. The figure given below, Fig. 4, shows the entity-

relationship diagram of this system. Here, there are 4 entities: admin, blockchain admin, police, and user. Each of the different entities has their own set of attributes related to them.

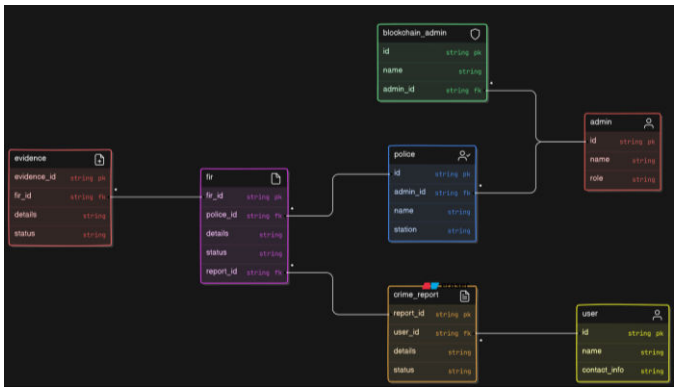

Fig. 4 Entity Relationship Diagram

D. Implementation

System requirements are the specifications of configurations a system must have in order to run the software successfully

1) Hardware Requirements

These are the required hardware for the implementation of this system:

- 1.8 GHz or faster processors
- 4 GB RAM or above; SSD with at least 5 GB of free space recommended
- 1 TB HDD or above
- 1024×768 Monitor Resolution

2) Software Requirements

- Frontend: HTML, JavaScript, Bootstrap
- Backend: Python, Django, Ethereum (for Blockchain), Solidity (for Smart Contracts)
- Database: MySQL

III. Results

After analyzing the proposed model, it was found that users (citizens and police officers) can register on the platform securely and add information on the system. It is then reviewed and once approved, officers can register FIRs, add evidences and they can't be edited at a later stage. Also, at least 3 blockchain admins have to approve FIRs for their final registration. If either one rejects, it cannot be registered on the system. Approval and rejection entries are marked in the blockchain ledger and subsequent blocks can also be viewed by the blockchain admins.

IV. Conclusion & Future scope

Blockchain enabled crime record management is a blockchain based document maintenance system which works under the principle of distributed network. In this system, the confidentiality and integrity of crime records and FIRs are maintained over a shared network. Each user can view the blockchain ledger by giving his user credentials. The smart contract is executed automatically when the blockchain condition occurred. This system has many advantages over normal document management system in such a way that it maintains transparency over the network. The blockchain ledger contains blocks of information which is linked together using fingerprinting. The fingerprinting is implemented using SHA256 hashing algorithm. Every block contains a set of valid transactions, the hash value of the block, the hash value of the previous block and proof of work. This makes the blockchain tamper proof and free from vulnerability.

Anything cannot be implemented in a single step. It is a fact that nothing is permanent in this world. So, this system also has some future enhancements in the booming and evergreen industry. Change is inevitable. Since web applications are subjected to change for each and every client, there is always a scope for further enhancements. The software was implemented and tested with real data and were found to be error free. Also, the system is protected from malicious users. However, as future work, some enhancements can be made in the way the blockchain key is generated.

References

[1] Pandian, Asha, Harsha, Ravuru Sai, Theja, Porachenu Ravi, Krishna, Tadavarthi Sai (2020), Crime Records Management System, *Journal of Computational and Theoretical Nanoscience*, 17 (8), 3653-3656

[2] Oludele Awodele, Onuiri Ernest E., Olaore Olufunmike A., Sowunmi Oluwawunmi O.Ugo-Ezeaba Anita A (2015), A Real Time Crime Records Management System for National Security Agencies, *European Journal of Computer Science and Information Technology*, 3 (2), 1-12

[3] Svedha K., Thiyagarajan A. (2020), A Real-Time Crime Records Management System, *International Research Journal of Engineering and Technology (IRJET)*, 7 (5), 7482-91

[4] Victoria Lemieux, Searching for Trust: Blockchain Technology in an Age of Disinformation, *Cambridge University Press*, May 2022

[5] Chelsea Palmer, Victoria Lemieux, Chris Rowell (2021), Multidisciplinary Blockchain Research And Design: A Case Study in Moving from Theory to Pedagogy to Practice, *International Conference on Information iConference 2021*, 12645, 587-602

[6] Leible Stephan, Schlager Steffen, Schubotz Moritz, Gipp Bela (2019), A Review on Blockchain Technology and Blockchain Projects Fostering Open Science, *Frontiers in Blockchain*, 2, 2-18

[7] Xu, M., Chen, X., Kou, G (2019), A Systematic Review of Blockchain, *Financial Innovation*, 5, 2-16

[8] Levis Daniel, Fontana Francesco, Ughetto Elisa (2021), A Look into the Future of Blockchain Technology, *PLoS One*, 16, 11

[9] Ćosić, Jasmin, Ćosić, Zoran, Bača, Miroslav (2011), An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence, *Journal of Information and Organizational Sciences*, 35 (1)

[10] Ahmad, Liza, Khanji, Salam, Iqbal, Farkhund, Kamoun, Faouzi (2020), Blockchain-Based Chain of Custody: Towards Real-Time Tamper-Proof Evidence Management, *ARES 2020: The 15th International Conference on Availability, Reliability and Security*, 1-8

[11] Maisha Tasnim, Abdullah Omar, Mohammad Rahman, Zakirul Bhuiyan (2018), CRAB: Blockchain Based Criminal Record Management System, *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, 294-303