iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.52548

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

FIR Security System Using Blockchain Technology

Divyaa. S. K[1], Kiruthika. K[2], Shahin Ashra. S[3], Sindhuja. J[4], Bhavani.N[5]
[1, 2, 3, 4]*Information Technology,* [5]*Associate Professor, Information Technology, Saranathan College of Engineering, Trichy, India*

Abstract: ***FIR (First Information Report) datamanagement is a critical task for law enforcement agencies to maintain law and order. Traditional FIR data management system often plagued by issues of data tampering, unauthorized access, and lack of transparency. In order to overcome this blockchain technology has been implemented which offers a decentralized, secure, and transparent solution to these problems. Storing FIR data on the blockchain can provide several advantages, including increased security, transparency, and immutability. Blockchain technology is a decentralized system that is resistant to modification, making it ideal for storing sensitive data such as FIR data. This system proposes a blockchain-based FIR data management system that utilizes smart contracts to automate the process of registering and accessing FIR data. The immutability of blockchain records can increase the reliability and trustworthiness of FIR data, while the decentralization of the blockchain ensures that there is no single point of failure. The user interface provides a graphical user interface for authorized users to interact with the system, Crime Investigators can view the data from database using their authentication credentials. Thereports, which are prepared by witnesses and police officers, are accessible to the investigator (admin).Investigators have the authority to edit data (i.e., update, remove, and so on), and this data aids investigators in speeding up their investigations and identifying offendersmore quickly. The evidences are secured using Block chain technology with SHA algorithm to create the hash values for each record. Secure cryptography functions to encrypt FIR information before storing on server has beenimplemented. The blockchain technology has the potential to revolutionize FIR data storage and improve the efficiency and effectiveness of law enforcement agencies.***

I. INTRODUCTION

FIR data management is an essential task for law enforcement agencies worldwide. FIR is the first official documents recorded by police when a crime is reported. These documents contain crucial information such as the victim's name, the accused name, the type of crime committed, the location of the crime, and other relevant details. FIR data is critical for investigations, evidence gathering, and judicial proceedings. Blockchain technology offers a decentralized, secure, andtransparent solution to store the FIR data. A blockchain collects information together in groups, known as blocks.Each block hold sets of information that are linked to the previously filled block,forming a chain of data known as the blockchain.

II. EXISTING SYSTEM

The existing methods store this FIR data in manualfilingand the e-copies are stored in centralized criminal record database. This does not ensure data security up to the mark. It could be tampered by third-party or evenpossibleto be changed by the police officers for their own benefit.

Disadvantage

Compromised FIR information may ultimatelyresult in favor of the criminal and a disgrace to our justicesystem.

III. PROPOSED SYSTEM

Blockchain technology offers a secure, andtransparent solution to these problems. Blockchain is a distributed ledger technology that allows data to be stored and managed securely and transparently without the need for a central authority. Blockchain technology offers several advantages over traditional data management systems, such as immutability, transparency, and security. The sensitive and crucial information contained in the FIR is stored in distributed database and is also encrypted making it not useful for the intruder even a database is compromised.

Advantages

Storing FIR data using blockchain makes it very difficult to alter or delete the record without leaving a trace, because of this we can prevent data tampering andmaintaining distributed database prevents data lossand also making it accessible from anywhere.

©IJRASET: All Rights are Reserved

A. Blockchain

Blockchain builds on the idea of P2P networks and provides a universal data set that every actor can trust, even though they might not know or trust each other. It provides a shared and trusted ledger of transactions, where immutable and encrypted copies of information arestored on every node in the network. Economic incentivesin the form of native network tokens are applied to make the network fault tolerant, and attack and collusion resistant. All network participants have equal access to the same data in real-time. Transactions running over thenetwork are transparent to all actors and can be traced back to their origin.

B. Storage Mechanism

A blockchain is a digital concept to store data.Theseblocks are chained together, and this makes their data immutable. When a block of data is chained to the other blocks, its data can never be changed again. It will bepublicly available to anyone who wants to see it ever again, in exactly the way it was once added to the blockchain. The most adopted secure algorithms associated with the blockchain technology are (SHA-1, SHA-2, and SHA-256) encryption because of their unique quality of hash functionthat creates unique outputs whengiven different inputs. The hash function here is a unique key created to identify atransaction that at the same timeidentifies an individual inthe chain.

C. Hashing

As the data blocks stored has distinct generated hash value mapped to them, these hashes are then linkedin an order of creation. These hash values are needed in the processes of retrieving the data blocks.
Here hashing is done by SHA-256 as it is considered as more secure algorithm than MD because this hash functions that do not have collusion problems anddeemedsecure otherwise, at least as yet.

1) *Blockchain headers:* Previous hash which locates the previous block's hash, Transaction details, Nonce which is an arbitrary number given by cryptography to differentiate the block'shash address.
2) *Hash Address:* Preceding hash, transaction details, and nonce aretransmitted through a hashing algorithm. This gives an output containing a 256-bit, 64 character length value, which is called the unique 'hash address.' Consequently, itis referred to as the hash of the block.
3) *Mining:* In Blockchain technology, the process of adding transactional details to the present digital/public ledger is called 'mining'. Mining involves generating the hash of a block transaction, which is tough to forge, therebyensuring the safety of the entire Blockchain without needing a central system.

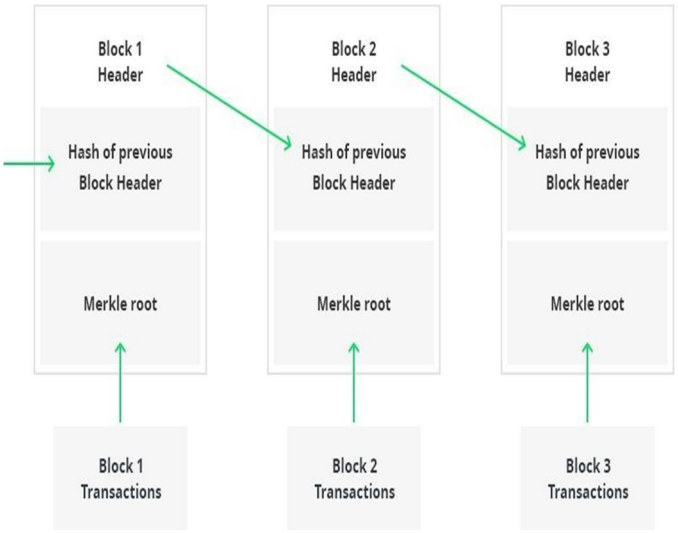


Fig.1 Data Storage

D. System Architecture

System architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal descriptionand representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.

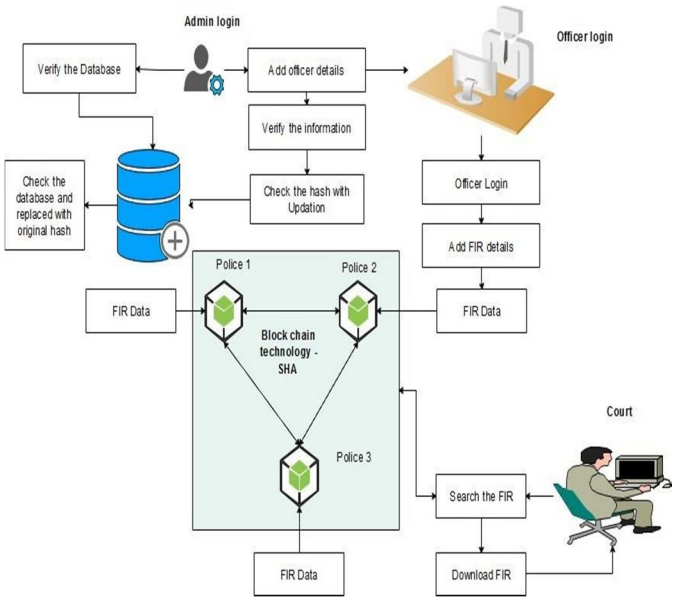


Fig.2 Architectural Diagram

E. Module DescriptionDemystifying Userroles

This system will incorporate three roles of user asin admin, officer who will the writer who files the FIR in police station, the court end whom have access to retrieve the stored FIR data. And also these ends need tobe access the data in a secure manner.

1) Entering Data Into The System

FIR data collection process is done by officer whohas authority to add FIR information. Each officer should have unique login factors. The authenticated officer can add FIR information regarding crime. Officer add the newFIR which contains the information such as station number, user name, FIR number, date, victim, witness, accused and FIR document.

2) Chaining Hashes

The uniquely generated hash of each data blocksusing SHA-256 hashing algorithm is chained ensuring thetransaction cannot be modified or tampered with. The modification will not be possible if the hash of the particular data block, to retrieve the hash value in the chain there is a need for the previous and the following hash value of blocks in the formed chain**.**

3) Data Retrieval

The stored FIR data needs to be retrieved by authorized personnel that is the court, court admin can login and search FIR data regarding inquiry process. It ensures the integrity and confidentiality of FIR data.

4) Overall Operation

A Block containing information about currenttransactions. Each data generates a hash. A hash is a string of numbers and letters. Transactions are entered in the order in which they occurred. The hash depends not only on the transaction but the previous transaction'shash. Even a small change in a transaction creates a completely new hash. The nodes check to make sure a transaction has not been changed by inspecting the hash.If a transaction is approved by a majority of the nodes then it is written into a block. Each block refers to the previous block and together make the Blockchain. A Blockchain is effective as it is spread over many computers, each of which has a copy of the Blockchain.

IV. IMPLEMENTATION

For the implementation, appropriate selection oflanguage is chosen and the design is transformed into working system.

Aim of the phase is to translate the design intoa best possible solution in a suitable programming language. This chapter covers the implementation aspects of the project, giving details of the programminglanguage and development environment used. It also gives an overview of the core modules of the project withtheir step by step flow.

©IJRASET: All Rights are Reserved

The implementation stage requires the following tasks.

1) Careful planning.
2) Investigation of the system and constraints.
3) Design of methods to achieve the changeover.
4) Evaluation of the changeover method.
5) Correct decisions regarding selection of theplatform

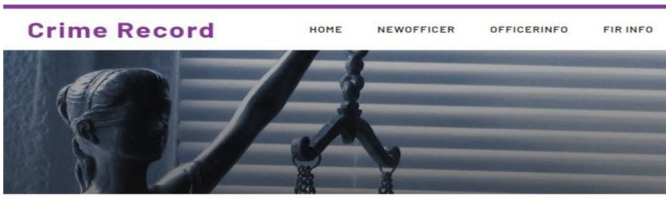
The front-end is developed using ASP.NET. With ASP.NET(Active Server Pages) and code-behind, the code and HTML can be isolated. It Utilize code to call local Windows APIs, use pre-constructed COM parts, and influence existing ActiveX controls to flawlessly coordinate existing applications and segments.

The backend uses SQL server for storing data in multiple instances. SQL Server scales from a portable tablet to symmetric multiprocessor frameworks.

V. EXPERIMENTAL RESULTS

All field entries must work properly. Pages must be activated from the identified link. The entry screen, messages and responses must not be delayed. Features to be tested:

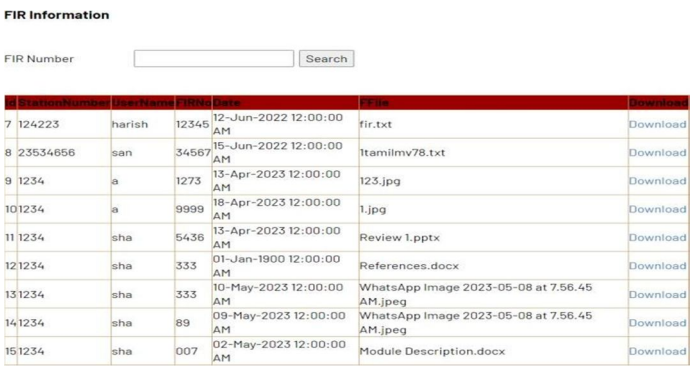
1) Verify that the entries are of the correct format.
2) No duplicate entries should be allowed.
3) Modification in any database entry should be verified for integrity with other database
4) instances for trustworthiness.
5) The uploaded relevant documents, photos andentered details should be stored properly.
6) No unauthorized access should be permitted.
7) All Admin features must work properly.
8) The court module must be able to retrieve thecorrect document using case ID.
9) The retrieved details must be properly decryptedfor readability.



id	FirstName	LastName	Mobile	Email	Address	Branch	StationNo	Username	Password
5	abinash	abinash	9486365535	abinash@gmail.com	no	Crime	23534845	abinash	abinash
6	harish	harish	09486365535	harish@gmail.com	no	Crime	124223	harish	harish
7	san	mani	09600357839	san@gmail.com	dgh	Crime	23534656	san	san
8	harish	harish	9600357839	harish@gmail.com	no 6 trichy	Crime	1234	harish	harish
9	sangeeth	Kumar	9600357839	sangeeth5535@gmail.com	dgh	Crime	12345	san	san
11	shahin	ash	9944110246	shahinashra19@gmail.com	TN	Women Safety	1234	sha	sha

Fig.3 Officers credentials

The credentials for appropriate police officers are createdby admin and provided to them using which they canenter reported FIR into our system.



id	StationNumber	UserName	FIRNo	Date	File	Download
7	124223	harish	12345	12-Jun-2022 12:00:00 AM	fir.txt	Download
8	23534656	san	34567	15-Jun-2022 12:00:00 AM	Itamilmv78.txt	Download
9	1234	a	1273	13-Apr-2023 12:00:00 AM	123.jpg	Download
10	1234	a	9999	18-Apr-2023 12:00:00 AM	1.jpg	Download
11	1234	sha	5436	13-Apr-2023 12:00:00 AM	Review 1.pptx	Download
12	1234	sha	333	01-Jan-1900 12:00:00 AM	References.docx	Download
13	1234	sha	333	10-May-2023 12:00:00 AM	WhatsApp Image 2023-05-08 at 7.56.45 AM.jpeg	Download
14	1234	sha	89	09-May-2023 12:00:00 AM	WhatsApp Image 2023-05-08 at 7.56.45 AM.jpeg	Download
15	1234	sha	007	02-May-2023 12:00:00 AM	Module Description.docx	Download

Fig.4 Uploaded FIRs

©IJRASET: All Rights are Reserved

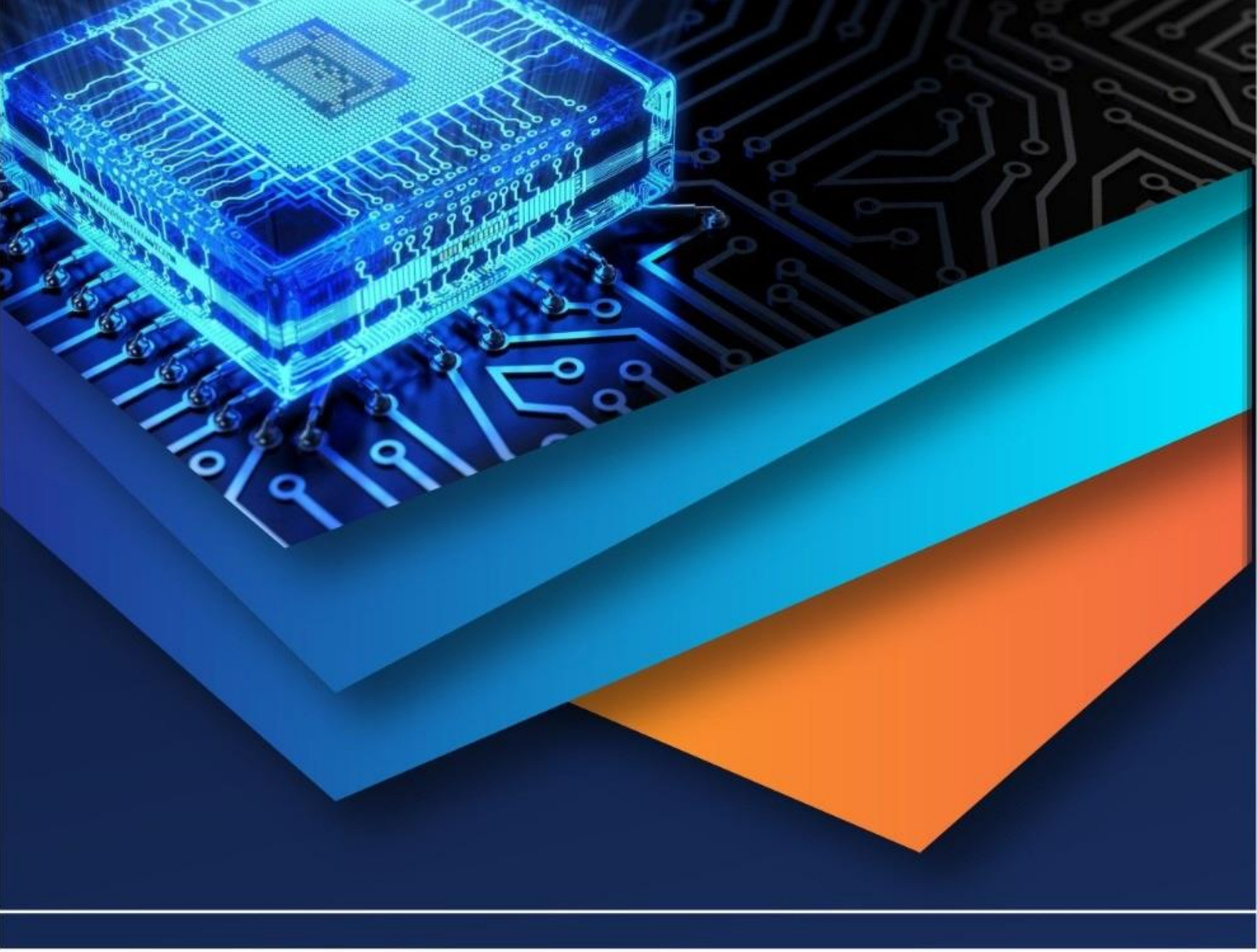
VI. CONCLUSION

The proposed blockchain-based FIR data management system offers several advantages over traditional FIR data management systems. It provides a secure, decentralized, and transparent solution to the problems of data tampering, unauthorized access, andlack of transparency. The system ensures data integrity, confidentiality, and authenticity while providing transparency and accountability to all stakeholders. This can impove the efficiency and effectiveness of FIR data management , thereby helping law enforcement agencies maintain law and order.

REFERENCES

[1] Al Omar, Abdullah, Abu Kaisar Jamil, Amith Khandakar, Abdur Razzak Uzzal, Rabeya Bosri, Nafees Mansoor, and Mohammad Shahriar Rahman. "A transparent and privacy- preserving healthcare platform with novel smart contract for smart cities." Ieee Access 9 (2021)
[2] Chen, Zerui, Youliang Tian, and Changgen Peng. "Anincentive-compatible rational secret sharing scheme using blockchain and smart contract. "Science China Information Sciences64 (2021): 1-21.
[3] Jyoti, Amrita, and R. K. Chauhan. "A blockchain and smartcontract-based data provenance collection and storing in cloud environment." Wireless Networks 28, no. 4 (2022): 1541-1562.
[4] A. Kumar, K. Abhishek, P. Nerurkar, M. R. Ghalib, A. Shankar, and X. Cheng, ``Secure smart contracts for cloud- based manufacturing using ethereum blockchain," Trans. Emerg. Telecommun. Technol., vol. 33, no. 4, p. 4129, Apr. 2022.
[5] T. Li, D. Li, and M. Wang, ``Blockchain-based fair and decentralized data trading model," Comput. J., vol. 65, no.8, pp. 2133_2145, Aug. 2021.
[6] T. Li, W. Ren, and Y. Xiang, `"FAPS: A fair, autonomous and privacy preserving scheme for big data exchange based on oblivious transfer, ether cheque and smart contracts," Inf. Sci., vol. 544, pp. 469_484, Feb. 2021.
[7] Lin, Chao, Debiao He, Xinyi Huang, and Kim-Kwang Raymond Choo. "OBFP: Optimized blockchain-based fair payment for outsourcing computations in cloud computing." IEEE Transactions on Information Forensics and Security16 (2021): 3241-3253.
[8] W. Xiong and L. Xiong, ``Anti-collusion data auction mechanism based on smart contract," Inf. Sci., vol. 555, pp.386_409, May 2021.
[9] Xuan, Shichang, Li Zheng, Ilyong Chung, Wei Wang, Dapeng Man, Xiaojiang Du, Wu Yang, and Mohsen Guizani. "An incentive mechanism for data sharing based on blockchain with smart contracts." Computers & Electrical Engineering 83 (2020): 106587.
[10] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, and Z. Weizhe, ``Blockchain-enabled decentralized trust management and secure usage control of IoT big data," IEEE Internet Things J., vol. 7, no. 5, pp. 4000_4015, May 2019

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)