WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

FIR Management System Using Blockchain Technology

Anusha S[1], Ambika P[2], Aishwarya NS[3], Apoorva[4], Bhavana V[5]

[1]Assistant professor department of computer science and engineering, MVJ College of engineering, India.
[2,3,4,5] Department of Computer science and engineering, MVJ college of engineering, India

ABSTRACT:

Police complaints need to be handled by a sophisticated and safe system immediately due to the rising rates of criminal activity and the continued use of antiquated complaint management procedures. In order to transform the way that police complaints are handled, this article presents a novel Blockchain-based approach. The suggested approach creates a decentralized platform that reduces the possibility of tampering and illegal access while guaranteeing the immutability and integrity of complaint recordings. The system ensures the legitimacy and timestamped submission of complaints through the use of blockchain hashing algorithms and encryption, contributing to the records' evidentiary value. The use of antiquated manual procedures is eliminated by this innovative method, enabling complainants to safely make complaints from a distance at any time. Additionally, by eliminating the risk of a single point of failure, the system's decentralized architecture strengthens the complaint handling procedure's robustness and level of trust. A transparent and accountable law enforcement environment is made possible by the revolutionary solution this research offers to the persistent problems in police complaint handling.

Keywords: Blockchain-based approach, Decentralized platform, Tamper-proof, Integrity, Legitimacy, Timestamped, Evidentiary value, Manual procedures elimination, Distance complaint submission, Accountable, Law enforcement.

Introduction:

In the current digital era, maintaining the timely and proper processing of judicial procedures is greatly dependent on the management of First Information Reports (FIRs). First Information Reports (FIRs) are the official records of a crime or incident, offering crucial information that forms the basis of any inquiry or legal action. However, issues with data security, integrity, and transparency frequently arise with traditional FIR management systems. The development of blockchain technology has completely changed how data is protected, accessed, and stored. Many of the drawbacks of conventional centralized databases can be solved by FIR management systems by utilizing the decentralized and irreversible features of blockchain technology. With the use of blockchain technology, FIR data may be stored on an open, unchangeable platform that guarantees its validity and integrity for the duration of the report's existence. The advantages of incorporating blockchain technology into FIR management systems are examined in this article. Law enforcement organizations, attorneys, and other stack holders can expedite the submission, retrieval, and updating of FIRs by harnessing the power of blockchain. Blockchain technology has the potential to improve the security, efficacy, and credibility of FIR management systems, which will ultimately result in more dependable and successful legal processes. This study attempts to demonstrate the revolutionary potential of blockchain in reinventing the handling and processing of First Information Reports (FIRs) through a thorough review of the capabilities and advantages of blockchain technology in FIR management. Organizations can guarantee the safe and transparent administration of First Information Reports (FIRs) by adopting blockchain technology, which will open the door to a more effective and reliable judicial system.

Large volumes of data, including FIRs, can be easily and scalablely stored on the cloud and accessed from any location with an internet connection. A more flexible, redundant, and economical FIR management system can be achieved by combining blockchain technology with cloud storage. The ability to safely store encrypted FIR data off-chain while keeping a reference to the data on the blockchain is a major benefit of combining cloud storage with blockchain technology. This hybrid strategy combines cloud storage's scalability and accessibility with blockchain's immutability and security. To further improve the overall security of FIR data, cloud providers frequently incorporate advanced security features including data encryption, access limits, and routine backups. Because cloud storage allows for seamless access to FIR data across many devices and locations, it can increase the efficiency of the FIR management system. This can make it easier for law enforcement organizations, attorneys, and other stack holders who handle FIRs to collaborate. Additionally, by offering automated backups and recovery methods, cloud storage can lessen the chance of data loss or corruption.

Methodology:

The proposed system is a decentralized one for managing the FIR with the help of blockchain technology. The detailed architecture of the system is explained as modules.

Security module:

Since the complaint transactions must be safeguarded, using a public blockchain is a bottleneck. Instead, a private blockchain has been employed. Our solution encrypts the information that has to be saved on the blockchain network for the registered complaint.

• A secret key is used to encrypt the complaint that is filed by a complainant. The security pin and open police station components are used to calculate the secret key.

• The grievance is appended to the blockchain upon registration. Utilizing the confidential key, the machine decodes the police complaint. This separates each complaint and lessens the burden on the blockchain. The public parts of the complainant's and the police officer's security pin are used to calculate the secret key.

• The policeman will handle the allegation and take appropriate action.

To guarantee the integrity and confidentiality of the complaint files, several procedures are put in place.

- Accessibility of Complaint Records
- Defined Blockchain by Users
- The MD5 Hashing Mechanism

Utilizing the RSA Algorithm for Private Key Generation

Blockchain module:

This module uses Java to implement a user-defined blockchain. The system's efficiency, security, and transparency are increased by the blockchain module's decentralized and immutable ledger for managing complaint files and related transactions.

An outline of the procedure for verifying blocks:

• Data Compilation: The block now contains the data.

• Hashing: Hashing is carried out following the registration of a complaint.

• Hashing Linking: A chain is formed by connecting each hashed block.

• Verification: A comparison between the hashed blocks and the earlier blocks is made. It is claimed that the data is unaltered if the hashes match.

• Block Addition: The block is appended to the blockchain following completion of the verification process.

Web Interface Module:

Users and police officers can upload and download files with ease thanks to the web interface's user-friendly interface. It is a platform for communication between the user and the system.

Numerous features are offered,

• User Registration: This allows the user to set up an account on the website.

• User Login: If the user has previously registered, they can access the portal by logging in with their login credentials.

• File Uploading: With this, users can attach a file containing photographs and personal information to their complaint.

• File Downloading: With this feature, the police officers can download the files.

• User Profile Management: This feature allows users to verify and amend their personal information.

Users and police officers can easily upload and download files, manage their profiles, and remain up to date by integrating a web interface into the system.

Cloud module:

This entails safely keeping all complaint-related data on a platform that runs on the cloud.

The police complaint management system can guarantee data availability, dependability, and accessibility from any location with an internet connection by utilizing cloud storage technology.

Features like data encryption, automatic backups, and access controls are available in cloud storage to improve the security and integrity of the data that is stored.

Streamlining the handling of First Information Reports (FIRs) and enhancing operational effectiveness in law enforcement agencies are made possible by the use of cloud storage modules.

Results:

The high degree of abstraction provided by the proposed system makes it a considerable advance over the current complaint handling system. By ensuring easy utilization for stakeholders, this abstraction also simplifies the user experience. The system is easy to use and doesn't require a lot of training for users, including police officers and complaint workers. File uploads, access management, and complaint monitoring are made simple by the system's user-friendly architecture. Higher user adoption, better police operational efficiency, and a user-centric complaint handling procedure are some benefits of the system's high degree of abstraction.

Fig.1-File uploading

Fig.2-File upload acknowledgement

Fig.3-File access control

Fig.4-Police registration

Fig.5-Available files for download

Fig.6-File download acknowledgement

Conclusion:

Using the power of cutting-edge technology, the project paper effectively provides a decentralized platform that transforms the handling of complaints. The suggested methodology assures efficiency, security, and transparency throughout the complaint handling process by combining blockchain and hybrid cloud.

By using blockchain technology, a transparent and unchangeable ledger is created, offering a trustworthy complaint history. Because of its immutability, stakeholders are more likely to trust and believe in the data's integrity. Furthermore, because the blockchain is decentralized, there is no longer a need for a central authority, which supports an impartial and equitable complaint resolution procedure.

A reliable and expandable storage option for complaint files is provided by the integration of hybrid cloud, more especially DriveHQ. By combining the benefits of public and private cloud services, this hybrid strategy ensures that storage is both accessible and safe.

Strict access controls prevent unwanted access or tampering, and authorized police personnel can simply retrieve and download files.

The user experience is prioritized in the developed architecture and modules, which offer a user-friendly interface and smooth functionality. By streamlining the complaint handling procedure, the technology increases productivity and efficiency for both police personnel and complainants. A fair and prompt resolution is made possible by the comprehensive approach, which guarantees that complaints are handled promptly and effectively.

All things considered, this project paper offers a novel and revolutionary approach to the complicated problems associated with complaint handling. Through the utilization of blockchain and hybrid cloud technologies, the suggested approach offers a safe, clear, and effective complaint management platform. The project has enormous potential to strengthen the procedures for resolving complaints and to promote accountability and trust within the system.

References

Research papers:

1. Aditya Vijaykumar Singh, Ashwin Omprakash Tiwari, Shreyash Sanjay Singh. 2022 6th International Conference on Trends in Electronics and Informatics(ICOEI). Date of Conference: 28-30 April 2022,Date Added to IEEE Xplore: 24 May 2022.
2. D. Song, A. Perrig, and D. Wagner, “Practical techniques for searches on encrypted data,” Proceeding 2000 IEEE Symposium on Security and
3. Privacy. IEEE, 2000, pp. 44–55.
4. J. Bethencourt, A. Sahai, and B.Waters, “Ciphertext-policy attribute-based encryption,” In Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.
5. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” IEEE 30th International Conference on Distributed Computing Systems. IEEE, 2010, pp. 253–262.
6. N. Premasathian and S. Choto, “Searchable encryption schemes: with multiplication and simultaneous congruences,” 2012 9th International ISC Conference on Information Security and Cryptology. IEEE, Tabriz, 2012,pp. 147–150.