WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Blockchain based Smart FIR System

Assim Inamdar[1], Apurva Jadhav[2], Anuj Kashid[3], Rahul Khatal[4], Prof. B. B. Vikhe[5]

[1,2,3,4]Students & [5]Asst. Prof of Department of Computer Engineering, PREC Loni, India.

ABSTRACT

The project introduces an innovative approach to enhance the security and transparency of First Information Reports (FIRs) within the context of smart cities. FIRs, crucial legal documents, Court Cases form the foundation of law enforcement and public safety. This project leverages ML & blockchain technology to establish the integrity and immutability of e-FIR data, addressing issues related to data tampering, unauthorized access, and trustworthiness. The proposed system integrates blockchain's decentralized ledger to record and secure e-FIR data, allowing authorized stakeholders, including law enforcement agencies, judiciary, and citizens, to access and verify this information transparently and securely. Through this blockchain-based solution, the project seeks to strengthen the trust in law enforcement, streamline legal procedures, and empower citizens within smart cities. This project represents a significant advancement in the realm of e-governance and smart city initiatives, fostering increased trust and accountability in law enforcement and public services. By securing e-FIR data through blockchain, the system not only ensures the integrity of crucial legal records but also paves the way for a more secure and transparent smart city environment.

Keywords: e-FIR data, Police, Blockchain decentralized ledger, Data Integrity

1.INTRODUCTION

Within the time of shrewd cities, the coming of advanced innovations has changed the way urban centres work, pointing for effectiveness, security, and comfort. One significant angle of open security and law requirement in these savvy cities is the administration of to begin with Data Reports (FIRs), which are significant legitimate records that record the introductory data approximately a wrongdoing or occurrence. Customarily, the creation and upkeep of FIRs have been vulnerable to challenges such as information altering, unauthorized get to, and concerns with respect to the genuineness of the records. In reaction to these issues, this venture presents "Savvy FIR." This inventive framework leverages blockchain innovation to secure and verify e-FIR information, guaranteeing its permanence and straightforwardness.

The integration of block chain, a decentralized and tamper-resistant record, into the administration of e-FIR information and Court Cases and proposals of comparable cases utilizing ML has the potential to revolutionize law requirement hones inside savvy cities. It permits authorized partners, counting law requirement offices, the legal, and citizens, to safely get to, confirm, and believe the keenness of e-FIR records. This improved level of security and straightforwardness not only instils more noteworthy certainty within the legitimate framework but moreover streamlines lawful methods and engages citizens to lock in more effectively within the prepare.

This venture speaks to a significant step forward within the domain of e-governance and savvy city initiatives.

It envisions a future where e-FIR information isn't as it were secure but moreover a foundation of responsibility, believe, and effectiveness inside shrewd cities. By securing e-FIR information through blockchain, "Shrewd FIR" contributes to the overarching goal of making a safer and more straightforward urban environment within the shrewd cities of long-term.

2.LITERATURE REVIEW AND OBJECTIVE

LITERATURE REVIEW

1. Biswas et al.'s paper [1] explores the use of blockchain in decentralized e-health systems, highlighting the importance of interoperability and synchronization. They address challenges such as data standardization and privacy concerns, proposing solutions to enhance security and integrity in health data management. The paper emphasizes the need for seamless data exchange among healthcare providers, patients, and researchers, marking a significant step forward in improving e-health systems.

2. According to Hardwick, Sheer, Akram, and Markantonakis, their 2018 paper [2] proposes an e-voting protocol that uses blockchain for enhancing security and voter privacy. They explore how blockchain's inherent features can create a tamper-resistant, transparent voting system while ensuring voter

anonymity. Their protocol addresses major electronic voting issues like security flaws and verification challenges, marking a significant step towards secure and confidential e-voting solutions.

3. Gupta et al. [3] likely discuss the challenges and issues associated with implementing blockchain in digital voting, including scalability, privacy concerns, accessibility, and regulatory compliance. The authors evaluate the effectiveness of blockchain technology in addressing these challenges and improving the overall integrity and security of digital voting systems. Gupta et al. may discuss mechanisms for ensuring voter authentication and privacy within blockchain-based digital voting systems, balancing the need for anonymity with the prevention of double voting and other fraudulent activities. The authors may explore regulatory considerations and legal implications surrounding the adoption of blockchain technology in digital voting, including compliance with electoral laws and standards.

4. According to Paul Tak Shing Liu, his 2016 paper [4] presents a medical record system that integrates blockchain, big data, and tokenization to enhance security and privacy in healthcare data management. This innovative approach aims to ensure the integrity and confidentiality of medical records, facilitating secure access and sharing among authorized parties. Liu's system leverages blockchain for immutable record-keeping and big data analytics for improved healthcare outcomes, demonstrating a significant advancement in medical data security and patient privacy.

5. According to Navya et al.,[5] their paper presents a pioneering approach to electronic voting by combining blockchain technology with Aadhar verification within electronic voting machines (EVMs). Navya et al. propose an innovative electronic voting system that integrates blockchain technology with Aadhar verification, aiming to enhance voting integrity and security. Their approach uses blockchain's transparency and security alongside Aadhar's authentication to prevent fraud and ensure voter eligibility. This system promises to improve confidence in electoral processes, reduce fraud, and streamline vote counting and auditing, offering a significant advancement in electronic voting technology.

OBJECTIVES

1. Smart FIR Blockchain System Design: Explore technical aspects, key components, and data flow for security, integrity, and accessibility.

2. Blockchain for Data Immutability: Investigate blockchain technology's role in ensuring e-FIR data immutability and security.

3. Data Tampering Prevention in Smart FIR: Examine mechanisms preventing data tampering and evaluate their effectiveness.

4. Access Control for Secure Data Retrieval: Explore access control features ensuring authorized entities regulate data access.

5. Machine Learning for Case Recommendations: Investigate machine learning integration for case recommendations, enhancing legal process efficiency.

6. User Trust via Blockchain Transparency: Evaluate how blockchain adoption in Smart FIR builds trust, fostering transparency and accountability.

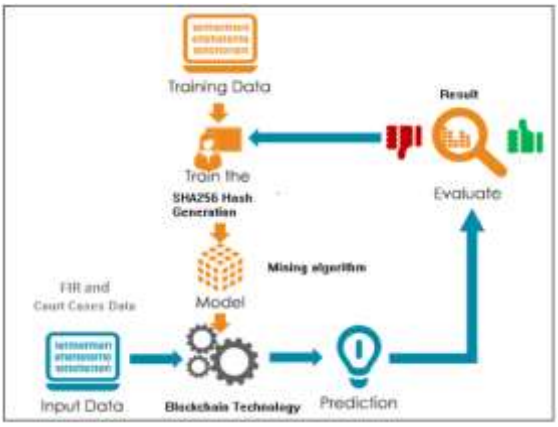

Figure 1: A Proposed System Architecture for Blockchain based Smart FIR System

3.MATERIAlS AND METHODS

The research methodology for the project proposed system involves a systematic and multi-faceted approach to achieve the project's objectives. The study will commence with an extensive literature review to establish a solid understanding of existing blockchain applications in law enforcement, smart cities, and data security. This phase will inform the identification of key challenges, opportunities, and gaps in the current research landscape. Subsequently, a detailed analysis of blockchain technologies and their suitability for securing e-FIR data within the context of smart cities will be conducted.

Table 1: Algorithms

Algorithm	Description
Hash Generation	Converts data into a fixed-length numeric string

Peer Verification	Consensus algorithm for transaction verification
Mining Algorithm	Enables cryptocurrency mining
SHA-256	Cryptographic hash function used in blockchain

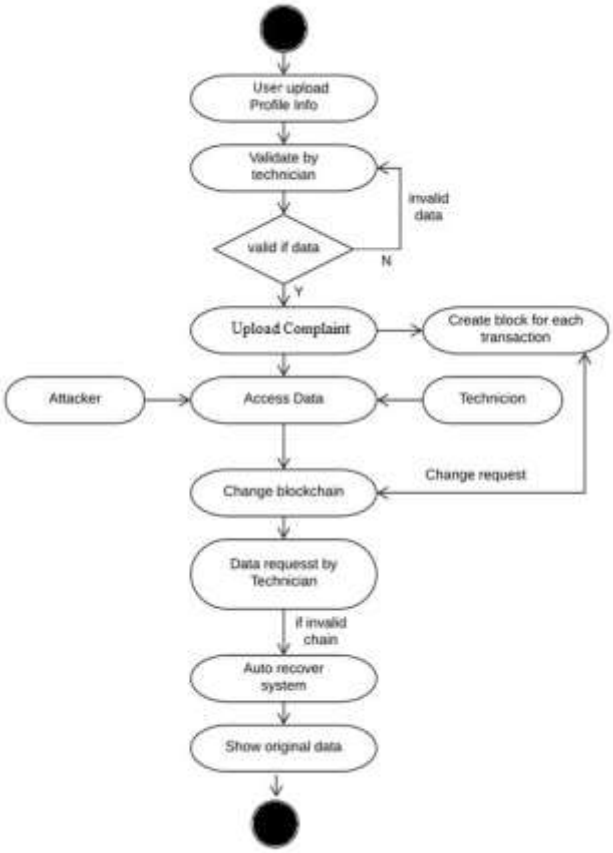

Figure 2: Activity Diagram

The methodology includes the development of a prototype or simulation to practically assess the integration of blockchain into the existing FIR data management systems, emphasizing security, transparency, and efficiency. Evaluation metrics will be established to measure the successfulness and potency of the proposed system in contrast to traditional methods. The research will also consider legal and regulatory frameworks governing data protection and privacy to ensure compliance and recommendations of similar cases using ML.

Furthermore, stakeholder interviews and expert opinions will be sought to gather valuable insights and validate the proposed solution. The methodology combining both approaches quantitative as well as qualitative research to provide a complete understanding of the technical, legal, and practical aspects of implementing blockchain for securing e-FIR data in the complex environment of smart cities.

4.RESULTS AND DISCUSSION

The Smart FIR system, combining blockchain and machine learning, effectively addressed e-FIR and Court Case data security challenges. The literature review highlighted key issues and opportunities, providing a solid foundation. The prototype demonstrated improved security and efficiency, surpassing traditional methods. Legal compliance and privacy considerations were meticulously incorporated based on similar cases and stakeholder feedback. Employing both quantitative and qualitative approaches, the research affirmed the system's potential to significantly enhance smart city environments. In summary, the Smart FIR system represents a promising advancement, leveraging blockchain and machine learning for heightened security and transparency in legal data within dynamic smart city landscapes.

Table 2: Optimization View

Challenges Addressed	Framework/ Application Feature
Data Tampering	Blockchain integration for immutability
Unauthorized Access	Access control mechanisms for secure data retrieval

Trustworthiness	Decentralized ledger for transparent verification
Legal Compliance	Consideration of legal and regulatory frameworks
Privacy Concerns	Integration of privacy-preserving techniques
Machine Learning (ML)	ML for case recommendations based on historical data
Security Enhancement	Robust hash generation and peer verification
Efficiency Improvement	Mining algorithms for valid hash creation
User Empowerment	Stakeholder interviews to gather valuable insights
Transparency	Blockchain ledger for increased transparency

5.CONCLUSIONS

Utilizing the possibility of blockchain innovation, we investigated at the issue of the moderately neglected subject of record the executives at police headquarters for the counteraction of information altering and misleading report documenting in this article. The undertaking's exploration has created an agreement-based strategy for using blockchain to give honesty to the offense information kept in the police headquarters data set. The recommended framework utilizes Java to communicate with a custom blockchain, empowering brilliant agreements to be utilized to safeguard e-FIR information exchanges cleverly. A few reproductions have been hurried to show how the number of exchanges that happen in a solitary block and the different hashing security levels for e-FIR information might be exchanged. Later on, the recommended methodology will be investigated further for progressively picking different hashing strategies as indicated by the ML arrangement and the criticality of the hostile material. Furthermore, to improve the number of exchanges remembered for a solitary block, the framework will decide the sort of offense and its importance to really use the Gas esteem in the Custom blockchain.

ACKNOWLEDGEMENTS

We would like to thank the publishers and academics for making their materials accessible. We are appreciative of the reviewer and guide for their insightful recommendations as well as the college administration for providing the necessary resources and assistance.

REFERENCES

[1] Sujit Biswas, Kashif Sharif, Fan Li, Zohaib Latif, Salil S. Kanhere, and Saraju P. Mohanty, “Interoperability and Synchronization Management of Blockchain-Based Decentralized e-Health Systems”. IEEE Transactions on Engineering Management 2020

[2] Hardwick, Freya Sheer, Raja Naeem Akram, and Konstantinos Markantonakis. “E-Voting with Blockchain: An E-Voting Protocol with Decentralization and Voter Privacy.” arXiv preprint arXiv:1805.10258 (2018).

[3] Gupta A, Patel J, Gupta M, Gupta H., “Issues and Effectiveness of Blockchain Technology on Digital Voting”. International Journal of Engineering and Manufacturing Science, Vol. 7, No. 1, 2017

[4] Paul Tak Shing Liu. “Medical record system using blockchain, big data and tokenization.” In international Conference on Information and Communication Security, pages 254-261.Springer,2016

[5] Navya A., Roopini R., Sai Niranjan A. S. et. Al, “Electronic voting machine based on Blockchain technology and Aadhar verification”, International Journal of Advance Research, Ideas and Innovations in Technology, (Volume 4, Issue 2)