*International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)*
*ISSN: 2456-236X*
*Vol. 09 Issue 01 | 2025*

# Blockchain-Based Digital Forensic Investigation and Evidence Protection System - Review

**Dr. Manjiri Karande[1], Ruchita Narkhede[2], Kajal Narkhede[3], Gaurav Chopade[4], Roshan Sawale[5].**

[1]Assistant Professor, Department of Computer Science & Engineering, Padm. Dr. V. B. Kolte College of Engineering, Malkapur, Maharashtra-443101

[2,3,4,5]Students of Department of Computer Science & Engineering, Padm. Dr. V. B. Kolte College of Engineering, Malkapur, Maharashtra-443101

## 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 ensure 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 trust in law enforcement, streamline legal procedures, and empower citizens within smart cities. This study 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, Court Case Data, crucial legal documents, e-governance and smart city, blockchain's decentralized ledger, etc.***

## 1. INTRODUCTION

In the era of smart cities, the advent of digital technologies has transformed the way urban centers function, aiming for efficiency, security, and convenience [8]. One pivotal aspect of public safety and law enforcement in these smart cities is the management of First Information Reports (FIRs), which are crucial legal documents that record the initial information about a crime or incident [9][10].

Traditionally, the creation and maintenance of FIRs have been susceptible to challenges such as data tampering, unauthorized access, and concerns regarding the authenticity of the records. In response to these issues, this project introduces "Smart FIR"[3][11]. This innovative system leverages blockchain technology to secure and authenticate e-FIR data, ensuring its immutability and transparency [12][13].

The integration of blockchain, a decentralized and tamper-resistant ledger, into the management of e-FIR data and Court Cases and recommendations of similar cases using ML has the potential to revolutionize law enforcement practices within smart cities. It allows authorized stakeholders, including law enforcement agencies, the judiciary, and citizens, to securely access, verify, and trust the integrity of e-FIR records. This enhanced level of security and transparency not only instills greater confidence in the legal system but also streamlines legal procedures and empowers citizens to engage more actively in the process.

This project represents a significant step forward in the realm of e-governance and smart city initiatives. It envisions a future where e-FIR data is not only secure but also a cornerstone of accountability, trust, and efficiency within smart cities. By securing e-FIR data through blockchain, "Smart FIR" contributes to the overarching goal of creating a safer and more transparent urban environment in the smart cities of the future.

## 2. RELATED WORK

The project encompasses a comprehensive exploration of the intersection between blockchain technology, smart cities, and law enforcement data security. Studies in blockchain applications in law enforcement have investigated its potential to enhance transparency, tamper-resistance, and authentication of records [14][15]. Within the broader smart city's paradigm, researchers have delved into integrating blockchain to bolster security and accountability in digital governance, with a specific emphasis on FIR (First Information Report) data [16][17]. The exploration extends to secure data storage solutions on blockchain, ensuring immutability and protection against unauthorized access for sensitive FIR records. Decentralized identity management solutions on blockchain are also considered to authenticate user identities securely. Privacy-preserving technologies, including zero-knowledge proofs, are explored to safeguard personally identifiable information within FIR documentation [18]. The legal implications of employing blockchain in law enforcement data management are studied, addressing compliance with existing

laws and standards. Additionally, investigations into the role of blockchain in digital forensics underscore its significance in maintaining forensic integrity, traceability, and non-repudiation in FIR-related data. The related works collectively contribute to insights crucial for implementing a secure and efficient e-FIR data management system leveraging blockchain within the dynamic landscape of smart cities.

The proposed work revolves around the development and implementation of a blockchain-based system, referred to as proposed work, designed to address the challenges associated with the security, integrity, and accessibility of crime investigation data & criminal cases data within the context of smart cities. This system will employ blockchain technology to create a decentralized ledger that records and secures crime investigation data, ensuring its immutability. Authorized stakeholders, including law enforcement agencies, the judiciary, and citizens, will have the capability to access and verify this data securely and transparently. The system will incorporate robust data tampering prevention mechanisms, safeguarding the integrity of investigation data records. Access control features will be implemented to ensure that only authorized individuals or entities can retrieve and authenticate the data. Through the adoption of blockchain technology, the project aims to instill greater trust in law enforcement procedures, streamline legal processes, and empower citizens to actively participate in their legal interactions. This comprehensive approach will contribute to the overarching goal of creating a more secure, accountable, and efficient smart city environment.

## 3. PROBLEM STATEMENT

In the evolving landscape of smart cities, the management and security of First Information Reports (FIRs) pose several challenges. FIRs are foundational legal documents that document the initial information regarding a crime or incident, serving as a critical part of law enforcement and public safety.

The problem statement addresses the need for a solution that can secure and authenticate e-FIR data, Court Cases, and recommendations of similar cases using ML guarantee its immutability and provide transparency and accessibility to authorized stakeholders within the framework of smart cities [19]. Such a solution is essential for bolstering trust, ensuring data integrity, and expediting legal procedures in the smart city environment.

## 4. PROPOSED SYSTEM

The proposed work revolves around the development and implementation of a blockchain-based system, referred to as "Smart FIR," designed to address the challenges associated with the security, integrity, and accessibility of e-FIR & Court Case data within the context of smart cities [6]. This system will employ blockchain technology to create a decentralized ledger that records and secures e-FIR data, ensuring its immutability [7]. Authorized stakeholders, including law enforcement agencies, the judiciary, and citizens, will have the capability to access and verify this data securely and transparently.

The system will incorporate robust data tampering prevention mechanisms, safeguarding the integrity of e-FIR records. Access control features will be implemented to ensure that only authorized individuals or entities can retrieve and authenticate the data. Through the adoption of blockchain technology and recommendations of similar cases using ML, the project aims to instill greater trust in law enforcement procedures, streamline legal processes, and empower citizens to actively participate in their legal interactions. This comprehensive approach will contribute to the overarching goal of creating a more secure, accountable, and efficient smart city environment.

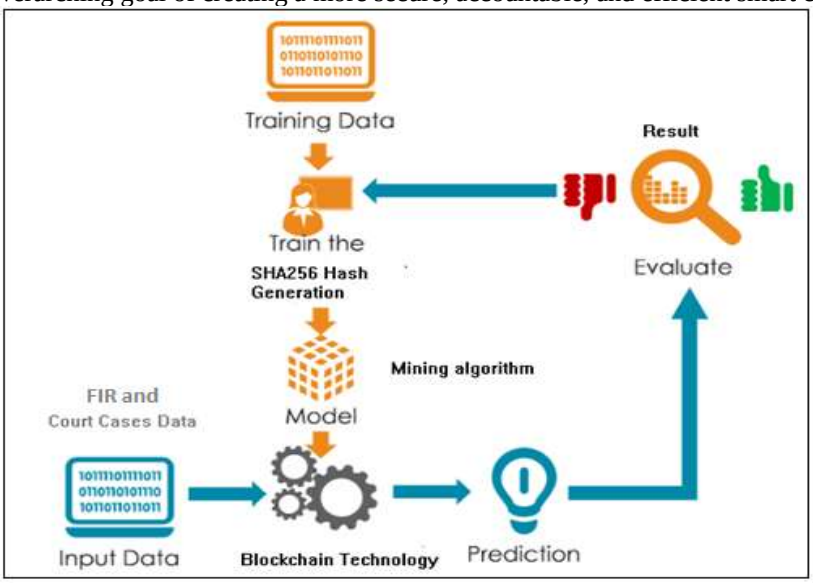


Fig.1: Proposed System Architecture

## 5. METHODOLOGY

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 [1][8]. 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. The methodology involves developing a prototype or simulation to evaluate the practical integration of blockchain into existing FIR data management systems, focusing on security, transparency, and efficiency. Evaluation metrics will be established to measure the effectiveness of the proposed system in comparison to traditional methods [9]. 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 integrates both quantitative and qualitative research approaches to provide a comprehensive understanding of the technical, legal, and practical aspects of implementing blockchain for securing e-FIR data in the complex environment of smart cities.

## 6. ALGORITHMS

**a) Hash Generation:**
A hash algorithm is a function that converts a data string into a numeric string output of fixed length. The output string is generally much smaller than the original data. ... Two of the most common hash algorithms are the MD5 (Message-Digest algorithm 5) and the SHA-1 (Secure Hash Algorithm) [10].
Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms.
**b) Protocol for Peer Verification:**
All peers on a blockchain network reach a consensus to verify transactions. This consensus is governed by an algorithm fed into the protocol layer of the blockchain. The blockchain gives all peers an identical copy of each transaction which eliminates trust thus making a trustless, distributed network [11].

**Input:** User gets IP address, User Transaction TID,
**Output:** Enable IP address or current query if any connection is valid
**Step 1 :** User generates any transaction DDL, DML or DCL query
**Step 2 :** Get a current IP address for each (read IP into IP address) If (connection (IP) equals(true)) Flag true Else Flag false End for
**Step 3:** if (Flag == true) Peer to Peer Verification valid Else Peer to Peer Verification Invalid End if End for

**c) Mining Algorithm for valid hash creation:**
Mining algorithms are the algorithms or functions that make the task of mining crypto-currencies possible.
Mining algorithms are the algorithms in charge of making possible cryptocurrency mining. Normally these algorithms are cryptographic hash functions very complex and they can adjust the mining difficulty [12]. A process that makes it more or less difficult for you to put together the puzzles that must be solved by the miners. This is to get miners to do complex computational work that, once solved, allows them to access a reward for that work.
**d) SHA-256**
With the birth of Bitcoin, SHA-256 became the first mining algorithm used in technology blockchain [13]. This is a powerful hash function. It serves multiple purposes within Bitcoin and virtually all existing cryptocurrencies. From ensuring the identification of each block, hashing addresses and other blockchain data, to serving as proof of work in mining, there is no doubt that SHA-256 is multifaceted.

## 7. CONCLUSION

In this paper, we have examined the challenge of the relatively under-developed area of record management in police stations for the prevention of data tampering and false report filing, using the concept of blockchain technology. Research conducted in this project has presented a consensus-based solution for providing integrity to the offenses data stored in police station database using blockchain.
In the proposed framework, Java is interfaced with Custom blockchain using Java to intelligently secure the e-FIR data transaction through smart contract. Multiple simulations have been performed to demonstrate the trade between numbers of transactions that occur in a single block and different hashing security levels for e-FIR data.
The proposed system will further be investigated in future for dynamically selecting different hashing algorithms based on ML classification and criticality of the offenses data. The system will also efficiently utilize the Gas value in the Custom blockchain by identifying the offense’s data type and its importance, in order to maximize the number of transactions stored in a single block.

## 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] Dongsheng Zhang. "Resilience enhancement of container-based cloud load balancing service". Technical report, PeerJ Preprints, 2018
[4] 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
[5] Navya A., Roopini R., SaiNiranjan 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)
[6] Panja, Somnath, and Bimal Kumar Roy. "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain."
[7] Martin A Makary and Michael Daniel. "Medical error-the third leading cause of death in the us". BMJ: British Medical Journal (Online), 353, 2016
[8] Till Neudecker, Philipp Andelfinger, and Hannes Hartenstein. "Timing analysis for inferring the topology of the bitcoin peer-to-peer network". In Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress, 2016 Intl IEEE Conferences, pages 358–367. IEEE, 2016
[9] Dongsheng Zhang and James PG Sterbenz. "Robustness Analysis and Enhancement of MANETs using Human Mobility Traces". Journal of network and systems management, 24(3):653–680, 2016.
[10] Paul Tak Shing Liu. "Medical record system using blockchain, big data and tokenization". In International Conference on Information and Communications Security, pages 254–261. Springer, 2016.
[11] Dongsheng Zhang and James P. G. Sterbenz, "Measuring the Resilience of Mobile Ad Hoc
[12] Networks with Human Walk Patterns", In Proceedings of the 7th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM), Munich, Germany, October 2015.
[13] Dongsheng Zhang and James P. G. Sterbenz. "Robustness analysis of mobile ad hoc networks using human mobility traces". In Proceedings of the 11th International Conference on Design of Reliable Communication Networks (DRCN), Kansas City, USA, March 2015.
[14] Dongsheng Zhang. "Resilience Evaluation and Enhancement in Mobile Ad Hoc Networks". PhD thesis, University of Kansas, 2015
[15] Dongsheng Zhang and James P.G. Sterbenz. "Modeling critical node attacks in MANETs". In Self-Organizing Systems, volume 8221 of Lecture Notes in Computer Science, pages 127–138. Springer Berlin Heidelberg, 2014
[16] Dongsheng Zhang and James P. G. Sterbenz. "Analysis of Critical Node Attacks in Mobile Ad Hoc Networks". In Proceedings of the 6th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM), pages 171–178, Barcelona, Spain, November 2014.
[17] Christian Decker and Roger Wattenhofer. "Information propagation in the bitcoin network". In Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on, pages 1–10. IEEE, 2013
[18] Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. C¸ etinkaya, and James P.G. Sterbenz. "Modelling Wireless Challenges". In Proceedings of the 18th ACM Annual International Conference on Mobile Computing and Networking (MobiCom), pages 423–425, Istanbul, August 2012.
[19] Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. C¸ etinkaya, and James P.G. Sterbenz. "Modeling Attacks and Challenges to Wireless Networks". In Proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM), pages 806–812, St. Petersburg, October 2012.