International Organization of Research & Development (IORD)
ISSN: 2348-0831
Vol 12 Issue 02 | 2025

Blockchain-Based Digital Forensic Investigation and Evidence Protection System

Dr. Manjiri Karande[1], Ruchita Narkhede[2], Kajal Narkhede[3], Gaurav Chopade[4], Roshan Sawale[5].
[1]Assistant Professor, Department of Computer Science & Engineering,
[2,3,4,5]Students of Department of Computer Science & Engineering,
Padm. Dr. V. B. Kolte College of Engineering, Malkapur, Maharashtra-443101

DOI: 10.5281/zenodo.14914160

ABSTRACT

This initiative presents a novel methodology to fortify the reliability and accountability of First Information Reports (FIRs) in smart city ecosystems. As foundational legal instruments, FIRs and court cases underpin law enforcement operations and community safety frameworks. By combining machine learning (ML) with blockchain technology, the system addresses vulnerabilities such as data manipulation, illicit access, and credibility gaps in digital FIR records. The framework utilizes blockchain's decentralized architecture to create tamper-proof audit trails for e- FIR data, enabling secure, real-time verification by authorized entities such as police departments, judicial bodies, and citizens. This approach aims to bolster public confidence in legal systems, simplify dispute resolution processes, and foster civic engagement in smart cities. By embedding e-FIR records into an immutable blockchain network, the project marks a transformative step in e-governance and urban digitization. It not only safeguards evidentiary integrity but also establishes a scalable model for transparent public service delivery. The integration of cryptographic security with automated ML-driven validations enhances operational efficiency while ensuring compliance with legal standards. Ultimately, this system redefines trust in civic institutions, laying the groundwork for safer, more equitable smart cities where governance and citizen empowerment converge.

Keywords: e-FIR data, Court Case Data, crucial legal documents, e-governance and smart city, blockchain's decentralized ledger, etc.

1. INTRODUCTION

In the age of smart cities, digital innovations have reshaped urban operations, prioritizing efficiency, security, and citizen-centric services [8]. Central to this evolution is the modernization of public safety mechanisms, particularly the handling of First Information Reports (FIRs)—critical legal documents that capture the initial details of criminal incidents or emergencies [9][10]. Historically, FIR management has been plagued by vulnerabilities such as data manipulation, unauthorized breaches, and disputes over record authenticity. To address these challenges, this project introduces Smart FIR [3][11], a groundbreaking framework that harnesses blockchain technology to safeguard and validate e-FIR data, guaranteeing its permanence, transparency, and resistance to alteration [12][13].

By embedding blockchain—a decentralized, tamper-evident ledger—into e-FIR systems and augmenting it with machine learning (ML) for case analysis and precedent recommendations, Smart FIR reimagines law enforcement workflows in smart cities. Authorized parties, including police departments, judicial authorities, and citizens, gain secure, real-time access to verified records, fostering trust in the system's integrity. This dual integration of blockchain and ML not only fortifies data security but also accelerates judicial processes, reduces administrative bottlenecks, and encourages civic participation in legal ecosystems. Beyond technical innovation, Smart FIR signifies a paradigm shift in e-governance and urban digitization.

It positions e-FIR data as a pillar of institutional accountability, bridging the gap between law enforcement efficiency and public trust. By ensuring cryptographic security and auditability, the system supports the broader vision of safer, more equitable smart cities where transparency and citizen empowerment drive civic progress.

2. RELATED WORK

This project conducts an in-depth analysis of the convergence of blockchain technology, smart city frameworks, and the security of law enforcement data. Prior research on blockchain applications in policing has highlighted its capacity to improve transparency, tamper-proof record-keeping, and authentication mechanisms [14][15]. In the context of smart cities, studies have examined the integration of blockchain to strengthen security and accountability in digital governance, particularly for safeguarding First Information Report (FIR) data [16][17]. Further exploration includes blockchain-based storage solutions to ensure the immutability of sensitive FIR records and prevent unauthorized access. Decentralized identity management systems are also evaluated to enable secure user authentication. To protect personal data within FIR documentation, privacy-enhancing tools such as zero-knowledge proofs are investigated [18]. The project further analyzes legal considerations tied to blockchain adoption in law enforcement data systems, focusing on alignment with regulatory frameworks. Additionally, research into blockchain's role in digital forensics emphasizes its utility in preserving integrity, traceability, and non-repudiation of FIR-related evidence. Together, these foundational studies inform the design of a robust, blockchain-driven e-FIR management system tailored for smart city ecosystems.

The proposed initiative focuses on creating a blockchain-powered platform to enhance the security, reliability, and accessibility of criminal investigation data within smart cities. By leveraging a distributed ledger, the system will ensure the permanent and unalterable storage of case records. Approved stakeholders—such as law enforcement, judicial bodies, and citizens—will gain secure, transparent access to verify and retrieve data through permissioned channels. The platform will integrate advanced safeguards against tampering while employing granular access controls to restrict data authentication to authorized users. By fostering transparency in policing workflows and simplifying judicial processes, this solution aims to strengthen public trust in legal systems. Furthermore, it seeks to empower citizens by enabling secure engagement with their case-related information. Through these measures, the system aspires to advance the development of smarter, more accountable urban environments anchored in operational efficiency and data integrity.

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.

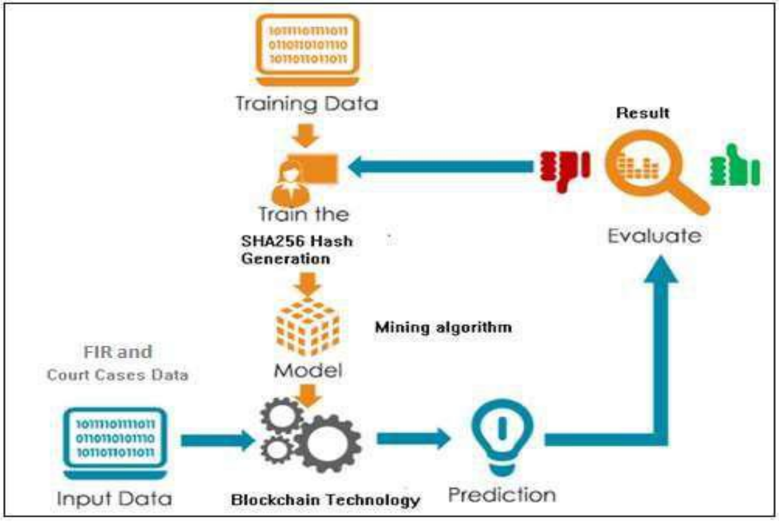


Fig.1: Proposed System Architecture

5. METHODOLOGY

The research methodology for the proposed system follows a structured and multi-dimensional approach to achieving the project's objectives. The study begins with an in-depth literature review to gain a comprehensive understanding of existing blockchain applications in law enforcement, smart cities, and data security [1][8]. This phase helps identify key challenges, opportunities, and gaps within the current research landscape. Following this, a thorough analysis of blockchain technologies will be conducted to assess their suitability for securing e-FIR data in the context of smart cities.

The methodology includes the development of a prototype or simulation to examine the practical integration of blockchain into existing FIR data management systems, with a focus on security, transparency, and efficiency. To assess the system's effectiveness compared to traditional methods, evaluation metrics will be defined and analyzed [9]. Additionally, legal and regulatory frameworks related to data protection and privacy will be examined to ensure compliance, along with the incorporation of machine learning-based recommendations from similar cases. Moreover, stakeholder interviews and expert consultations will be conducted to gather valuable insights and validate the proposed solution. This methodology combines both quantitative and qualitative research approaches to offer a well-rounded perspective on the technical, legal, and practical aspects of implementing blockchain for securing e-FIR data in the complex landscape 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.

```
Input: Genesis block, Previous hash, data d, Output: Generated hash H according to given data
Step 1 : Input data as d
Step 2 : Apply SHA 256 from SHA family
Step 3 : CurrentHash= SHA256(d) Step 4 : Retrun CurrentHash
```

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 get IP address, User Transaction TID,
Output: Enable IP address or current query if any connection is valid
Step 1 : User generate the any transaction DDL, DML or DCL query
 Step 2 : Get 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.

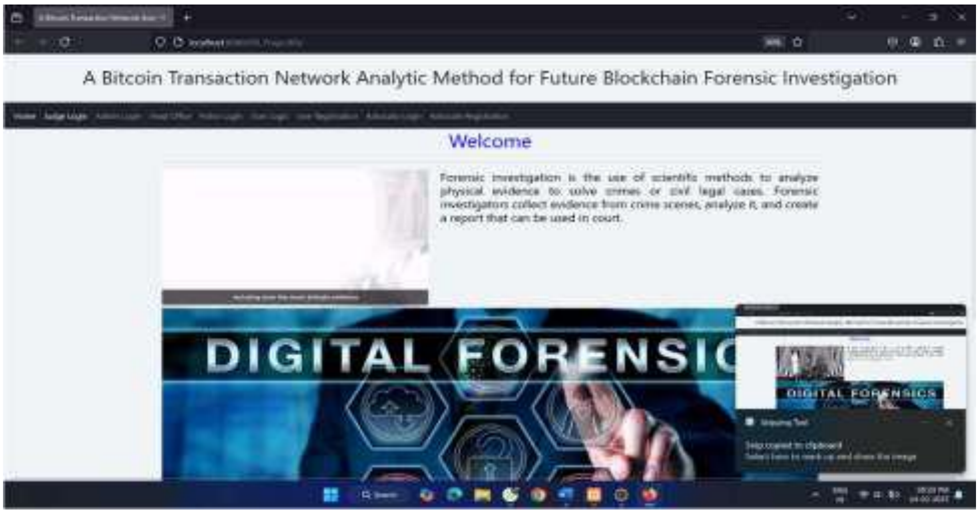
```
Input: Hash Validation Policy P[], Current Hash Values hash Val
Output: Valid hash
Step 1 : System generate the hash Val for I th transaction using Algorithm 1
Step 2 : if (hash Val.valid with P[]) Valid hash Flag =1 Else Flag=0 Mine again randomly
Step 3 : Return valid hash when flag=1
```

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.

```
MessageDigest md = MessageDigest.getInstance("SHA-1"); byte[] messageDigest =
md.digest(input.getBytes()); BigInteger no = new BigInteger(1, messageDigest);
String hashtext = no.toString(16);
while (hashtext.length() < 32) { hashtext = "0" + hashtext;   }
return hashtext;  }
catch (NoSuchAlgorithmException e) { throw new RuntimeException(e);  }
```

7. RESULTS AND DISCUSSION

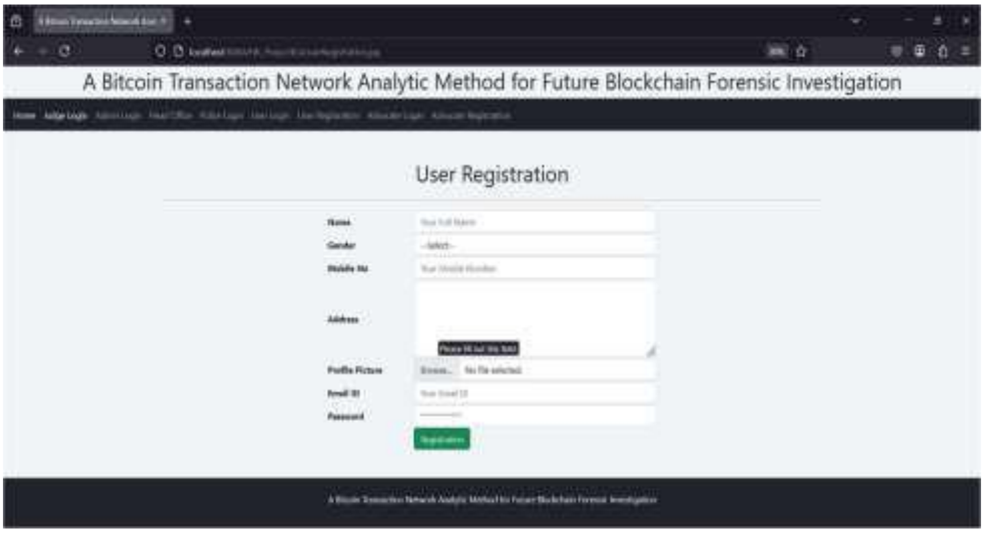


A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

Welcome

Forensic investigation is the use of scientific methods to analyze physical evidence to solve crimes or civil legal cases. Forensic investigators collect evidence from crime scenes, analyze it, and create a report that can be used in court.

Fig 2 A : Home Screen



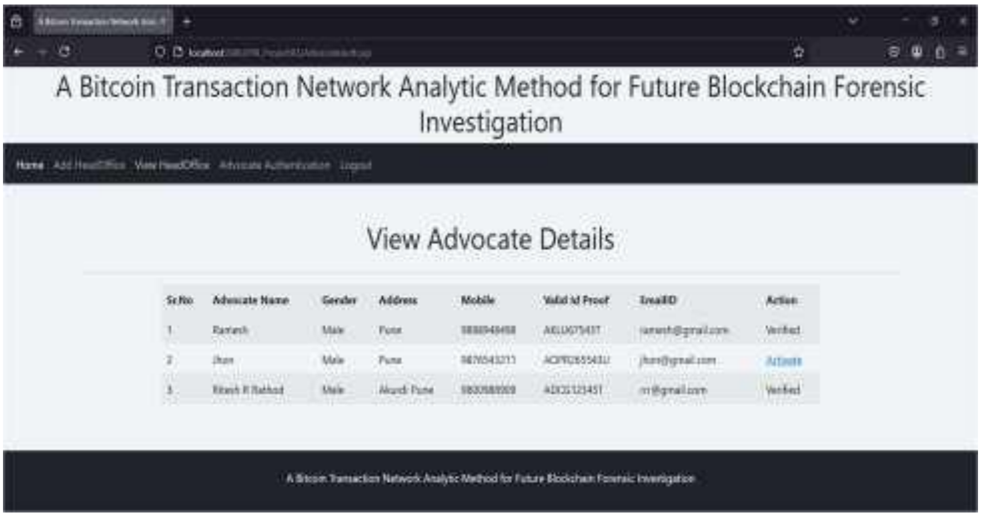
A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

User Registration

Name	Your Full Name
Gender	--Select--
Mobile No	Your Mobile Number
Address	
Profile Picture	No file selected.
Email ID	Your Email ID
Password	

A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

Fig 2 B : User Registration Form



A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

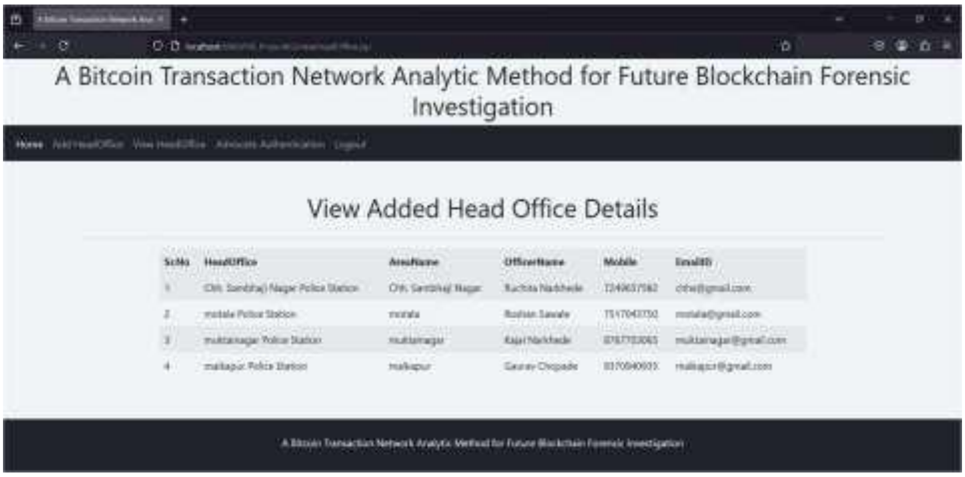
View Advocate Details

Sr.No	Advocate Name	Gender	Address	Mobile	Valid Id Proof	EmailID	Action
1	Ramesh	Male	Pune	9888949458	AKLUG7543T	ramesh@gmail.com	Verified
2	Jhon	Male	Pune	9876543211	ACPPD2655431J	jhon@gmail.com	Activate
3	Ritesh R Rathod	Male	Akurdi Pune	9800988909	ADCG123451	rr@gmail.com	Verified

A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

Fig 2 C : Advocate Authentication

DOI: 10.5281/zenodo.14914160



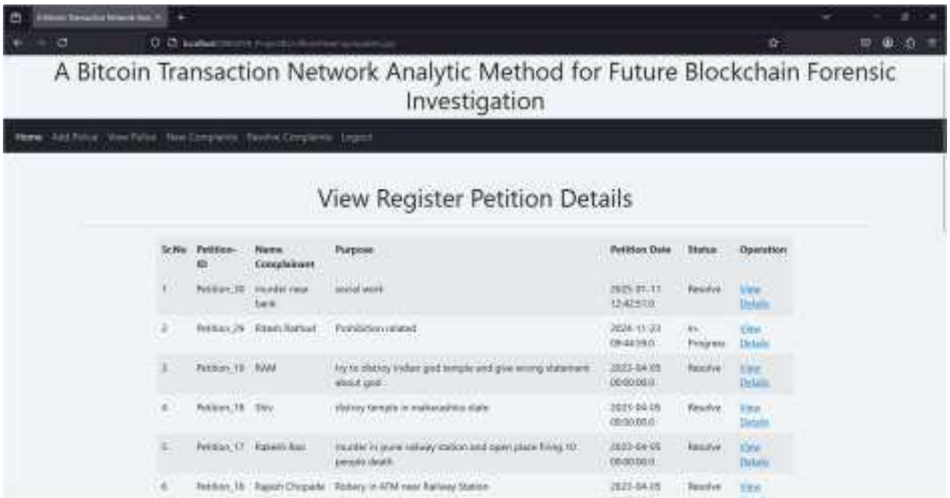
A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

View Added Head Office Details

Sr.No	HeadOffice	AreaName	OfficerName	Mobile	EmailID
1	Chh. Sambhaji Nagar Police Station	Chh. Sambhaji Nagar	Ruchita Narkhede	7249637582	chhs@gmail.com
2	motala Police Station	motala	Roshan Sawale	7517043750	motala@gmail.com
3	muktainagar Police Station	muktainagar	Kajal Narkhede	8767703065	muktainagar@gmail.com
4	malkapur Police Station	malkapur	Gaurav Chopade	8370840935	malkapur@gmail.com

A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

Fig 2 D : Head Office Details

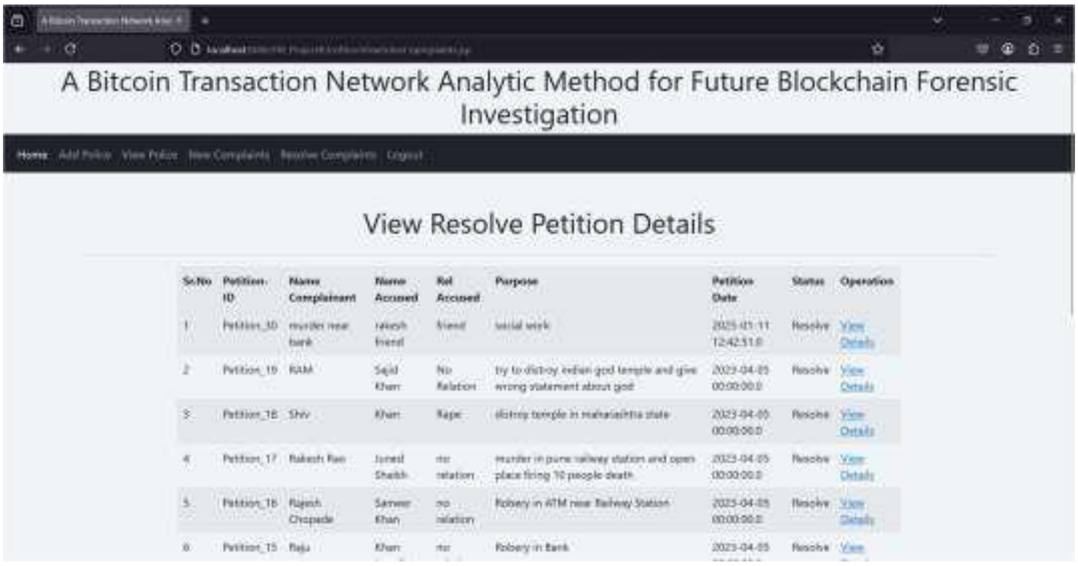


A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

View Register Petition Details

Sr.No	Petition-ID	Name Complainant	Purpose	Petition Date	Status	Operation
1	Petition_30	murder near bank	social work	2025-01-11 12:42:51.0	Resolve	View Details
2	Petition_29	Ritesh Rathod	Prohibition related	2024-11-23 09:44:59.0	In Progress	View Details
3	Petition_19	RAM	try to distroy indian god temple and give wrong statement about god	2023-04-05 00:00:00.0	Resolve	View Details
4	Petition_18	Shiv	distroy temple in maharashtra state	2023-04-05 00:00:00.0	Resolve	View Details
5	Petition_17	Rakesh Rao	murder in pune railway station and open place firing 10 people death	2023-04-05 00:00:00.0	Resolve	View Details
6	Petition_16	Rajesh Chopade	Robery in ATM near Railway Station	2023-04-05	Resolve	View

Fig 2 E : View Register Petition Details



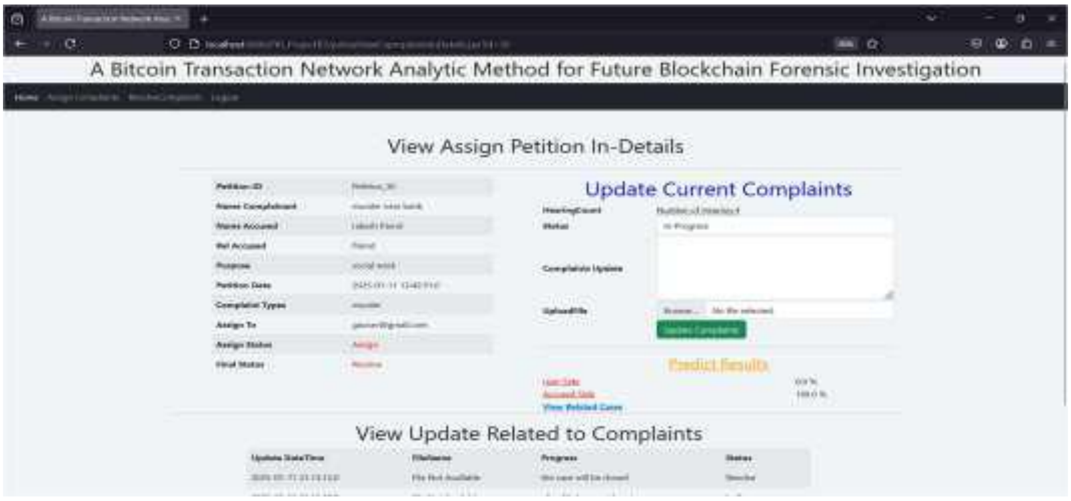
A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

View Resolve Petition Details

Sr.No	Petition-ID	Name Complainant	Name Accused	Rel Accused	Purpose	Petition Date	Status	Operation
1	Petition_30	murder near bank	rakesh friend	friend	social work	2025-01-11 12:42:51.0	Resolve	View Details
2	Petition_19	RAM	Sajid Khan	No Relation	try to distroy indian god temple and give wrong statement about god	2023-04-05 00:00:00.0	Resolve	View Details
3	Petition_18	Shiv	Khan	Rape	distroy temple in maharashtra state	2023-04-05 00:00:00.0	Resolve	View Details
4	Petition_17	Rakesh Rao	Juned Shaikh	no relation	murder in pune railway station and open place firing 10 people death	2023-04-05 00:00:00.0	Resolve	View Details
5	Petition_16	Rajesh Chopade	Sameer Khan	no relation	Robery in ATM near Railway Station	2023-04-05 00:00:00.0	Resolve	View Details
6	Petition_15	Raju	Khan	no	Robery in Bank	2023-04-05	Resolve	View

Fig 2 F : View Resolve Petition Details

DOI: 10.5281/zenodo.14914160



A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

Home Assign Complaints [illegible] Logout

View Assign Petition In-Details

Petition ID	[illegible]
Name Complainant	[illegible]
Name Accused	[illegible]
Rel Accused	Friend
Purpose	social work
Petition Date	[illegible]
Complaint Types	murder
Assign To	[illegible]
Assign Status	Assign
Final Status	Resolve

Update Current Complaints

HearingCount	[illegible]
Status	In Progress
Complaints Update	
UploadFile	Browse... No file selected.

Update Complaints

Predict Results

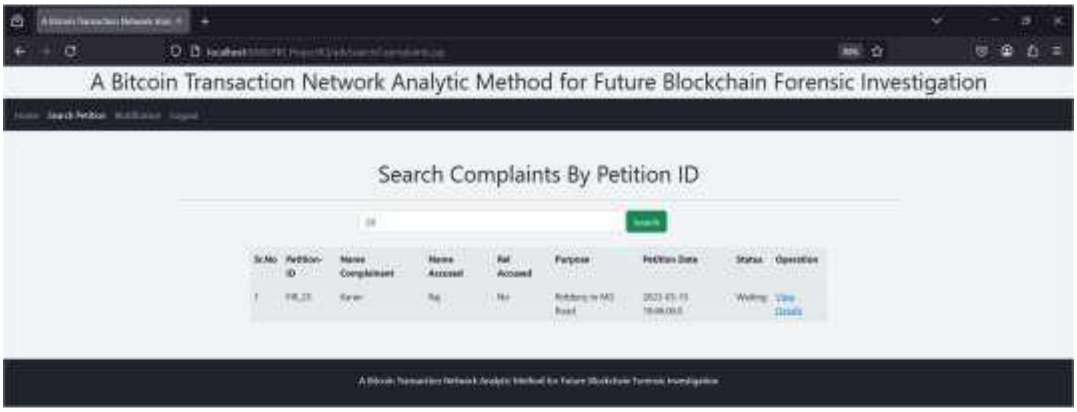
[illegible]	[illegible]
[illegible]	[illegible]

View Related Cases

View Update Related to Complaints

Update Date/Time	FileName	Progress	Status
[illegible]	File Not Available	the case will be closed	[illegible]

Fig 2 G : View Assign Petition In-Details



A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

Home Search Petition Notification Logout

Search Complaints By Petition ID

[illegible] Search

Sr.No	Petition-ID	Name Complainant	Name Accused	Rel Accused	Purpose	Petition Date	Status	Operation
1	[illegible]	Karan	Raj	No	Robbery in MG Road	[illegible]	Waiting	View Details

A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation

Fig 2 H : Search Complaints by Petition ID

8. CONCLUSION

we implemented and evaluated a blockchain-based framework for securing record management in police stations, with a focus on preventing data tampering and false report filing. The proposed system integrates Java with a custom blockchain to ensure the integrity of e-FIR data transactions through smart contracts. Through multiple simulations, we analyzed the trade-offs between the number of transactions per block and the impact of different hashing security levels on data protection. Our findings indicate that the system effectively enhances data security while maintaining efficiency in blockchain storage. Additionally, the results suggest that dynamically selecting hashing algorithms based on machine learning classification and the criticality of offense data can further optimize system performance. Future work will focus on refining the framework by implementing an adaptive mechanism for selecting hashing techniques and efficiently managing Gas values in the custom blockchain to maximize storage utilization while preserving data integrity.

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 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.

[12] 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.

[13] Dongsheng Zhang. “Resilience Evaluation and Enhancement in Mobile Ad Hoc Networks”. PhD thesis, University of Kansas, 2015

[14] 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

[15] 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.

[16] 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

[17] 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.

[18] 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.