FIR-Chain: Blockchain based First Information Report System

Harshvardhan More
Computer Engineering, SIGCE, Mumbai
University, Ghansoli, Maharashtra, India

Adi Shettiar
Computer Engineering, SIGCE, Mumbai
University, Ghansoli, Maharashtra, India

Shivani Pawar
Computer Engineering, SIGCE, Mumbai
University, Ghansoli, Maharashtra, India

Prof. Selvamurugan Kasi
Computer Engineering,SIGCE, Mumbai
University, Ghansoli, Maharashtra, India

***Abstract*—India is experiencing a sharp rise in criminal activity. This is a serious problem, as many of these crimes go unreported. Although there is an online platform for the police to store First Information Reports (FIR) and Non-Cognizable Reports (NCR), most FIRs are still written by hand. This is inefficient and can lead to errors. Additionally, the complainant must typically be at the police station to report a cognizable offense. This can be inconvenient and time-consuming, especially for victims who live in rural areas. In 2009, the Crime and Criminal Tracking Network and Systems (CCTNS) were launched as an efficient e-governance system. This system has helped to improve the reporting of crimes, but it is still a centralized system. This means that it is vulnerable to cyberattacks and can be easily shut down by a single point of failure. Therefore, a fully decentralized system is required to ensure no single point of failure and that complaints are handled safely and securely to prevent unauthorized access. This paper proposes a blockchain-based solution called FIR-CHAIN to manage complaints against cognizable and non-cognizable offenses. Using this system, complaints can be registered by users. The police stations will be able to see complaints registered in their jurisdiction, register FIRs/NCRs accordingly, and act on them. Through a prototype implementation using Go- Ethereum (Geth), smart contracts, and Node web server, we demonstrate the practical use of FIR-CHAIN. We show that our system can be easily used by users, police personnel, and Higher Authorities to improve the current systems in India.**

***Index Terms*—Blockchain, Authentication, FIR, IPFS, Ethereum, Smart contracts, Geth**

I. INTRODUCTION

There are two types of offenses in India: cognizable and non-cognizable [1]. A cognizable offense is a serious crime that the police can investigate and arrest suspects without a warrant. The police do not need permission from the court to investigate a cognizable offense. Sometimes, the police must file an FIR when they receive information about a cognizable offense. However, the police can also investigate a cognizable offense without filing an FIR. Cognizable offenses are often more severe crimes, such as murder, theft, and kidnapping, violent or involving property damage. They are also often not bailable, meaning suspects cannot be released from jail until their trial ends. As Section 2 (c) of the Criminal Procedure Code 1973 [2] defines, Police can arrest suspects of cognizable offenses without a warrant.

Non-cognizable offenses are less severe crimes, such as public nuisance and petty theft. It is a less serious crime that The police cannot investigate or arrest suspects for without a warrant. The police can only investigate a non-cognizable offense if they have a warrant from the court. They are also often bailable, meaning suspects can be released from jail until their trial ends. Police cannot arrest suspects of non-cognizable offenses without a warrant.

The term “First Information Report” refers to a report of information that, for whatever reason, reaches the police first in time. The victim of a cognizable offense or someone acting on their behalf typically files a complaint with the police. It is necessary to register an FIR [1] at the police station in the area where the offense was committed. When the police learn about the commission of a crime that can be prosecuted, they create a written report called an FIR. Corruption in the police force is a significant obstacle to justice. In a recent study [3], 24% of people who tried to report a crime to the police were unable to do so. Of those who could report a crime, 30% did not receive a copy of the FIR.

A. Who can lodge an FIR?

Anyone can lodge an FIR in India, not just the victim of the crime [2]. An FIR is a First Information Report, the first step in the criminal justice process. It is important to note that an FIR is not the same as a charge sheet, a document filed by the police after they have completed their investigation. The following people can lodge an FIR:

- The victim of the crime.
- A witness to the crime.
- A police officer who learns of the crime.
- A person who knows about the crime.

The police must register an FIR if they receive information about a cognizable offense. A cognizable offense is an offense that is serious enough for the police to arrest the accused without a warrant. If the police refuse to register an FIR, the person who lodged the FIR can file a complaint with the Superintendent of Police (SP) or the Deputy Commissioner of Police (DCP). The SP or DCP can then order the police to register the FIR. The accused will then defend themselves in court. Some of the benefits of lodging an FIR:

[1] https://ncrb.gov.in/sites/default/files/IIF.pdf
[2] https://www.legalserviceindia.com/legal/article-1329-how-to-file-an-html

- It starts the criminal justice process.
- It can help to protect the victims and witnesses.
- It can help to recover property that was stolen.
- It can help to bring the accused to justice.

In FIR-Chain, Users and Police personnel will be authenticated for their roles using our other work, Auth Block, a blockchain based authentication framework. Users will register the com- plaint on the system. The Police personnel will then check the details and act accordingly. They will have to update the action details on the system. These details will help the user track the progress of the complaint. The complaint, including the timestamp, is stored on the blockchain network. If the police do not file an FIR or claim that they never received a complaint, the complainant will have strong evidence against them because all entries are stored in an immutable database. This means that the data cannot be changed or deleted, so there is no way for the police to tamper with the records. Go- Ethereum (Geth) [3] is used to create a local blockchain network. A web server is created using the Django framework which is a User Interface and connects blockchain to the front end. Various smart contracts are created according to the modules which are explained in detail in later sections.

The rest of the paper is organized as follows: Section II describes all the literature work available in this domain, and the main differences between traditional and blockchain based systems. It concludes with the issues in current systems, emphasizing the motives of this work. Section III proposes FIR-Chain: A blockchain based FIR system and explains it design. Sections IV explain the implementation of various modules of FIR-Chain in detail. Section V describes the results and analysis of the system on various parameters and its comparison with literature works. Section VI concludes the work with discussion and future scope.

II. Related Work

The authors in [4] discussed a method for securing online FIRs using blockchain. The authors proposed a system for registering complainants, suspects, and witnesses. The pre-registration process of an FIR is conducted by the officer in charge, and the user credentials are stored in a local database. This means that someone could potentially prevent an FIR from being registered by making changes to the user authentication data. Additionally, the authors did not address the issue of false FIRs, which is a potential concern. In their paper, [5] proposed a blockchain-based system for storing criminal data. The system uses a distributed ledger to store the data, which makes it more secure and resistant to tampering. The system also uses a pre-registration process to ensure only authorized users can access the data. However, the authors did not address the issue of the integrity of user data stored on the cloud database. This could allow someone to tamper with the data, leading to false FIR registrations. The system allows only authorized users, like courts and various agencies, to access criminal data. Other users, such as individuals, airports, and visa application centers, can access the data when needed. In [6], authors have proposed a web-based FIR system. The system allows users to file FIRs online, and the administrator ensures the authenticity and integrity of the data by only filing the pre-registered FIR in the local database. This provides efficiency and transparency. But the authors did not address the integrity of data issue even if they used the pre-registering technique.

The paper [7] examines the use of blockchain technology to improve record management in police stations. They propose a solution that stores the hash of the FIR (First Information Report) on the blockchain, but the FIR remains in the local database. This means that any changes to the FIR will be detectable, but the original data will not be recoverable. It argues that this solution can help prevent data tampering and false reporting, both serious problems in police stations. Data tampering can occur when someone changes or deletes records to cover up wrongdoing. False reporting occurs when someone files a false report with the police to gain an advantage or to harm someone else. It concludes that blockchain technology has the potential to improve record management in police stations and to help to prevent data tampering and false reporting.

The authors of [8] propose a new method for registering FIRs using consortium blockchain technology. Their method simplifies and speeds up the registration process using a Proof of Vote consensus algorithm. However, their method doesn't explain how FIRs are exactly stored on the blockchain, and they don't allow the uploading of document proofs to the blockchain. Authors of [9] proposed a new application that would allow individuals in Riyadh to report and manage their complaints more effectively. The system would allow people to register complaints, which would then be helpful to the police department in identifying criminals. The application's main goal is to improve the efficiency and effectiveness of communication between police officers and the public. The application would also be a valuable tool for tracking and monitoring criminals across the country. It would provide a complete online record of crime-related information, including the criminals' names, descriptions, criminal histories, and crimes they have committed. The authors of BlockIPFS [10] proposed a blockchain based interplanetary file system (IPFS) for forensic and trusted data traceability. It builds on IPFS by adding blockchain technology to create a clear audit trail. In [11], proposed a decentralized system for storing citizen Criminal records using a permissioned blockchain. This allows for improved data integrity and accessibility, as well as reduced costs associated with traditional record keeping methods. This system takes advantage of some of the blockchain's properties, such as privacy, security, immutability, and accountability, to ensure the safety and integrity of sensitive data.

A. Background of Police systems in India

Tamil Nadu has launched the Criminal Automated Admin- situation and Retrieval of Useful Statistics (CAARUS) project, which aims to improve the efficiency of the police investigation

[3] https://geth.ethereum.org/

and record keeping. Karnataka has launched Police IT project [4], which aims to provide all police stations with computers and internet access. The National Crime Records Bureau (NCRB) launched the Common Integrated Police Application (CIPA) in 2004. CIPA is a software application that helps police officers to manage their work. It is built on a client-server architecture on a NIC Linux platform using Java and Postgres SQL database. The Crime and Criminal Tracking Network Systems (CCTNS) [5] is a mission mode project under the National e-Governance Plan (NeGP) of the Government of India. It aims to enhance the efficiency and effectiveness of policing by adopting e-governance principles. CCTNS builds on the foundation of CIPA and expands its functionality to include a wider range of police activities.

B. *Issues with current systems*

There are several problems that people face in registering FIRs in India. These may be related to the practical side of the current system, or they may be due to the technical side of the systems used to register e-FIR. Some of these problems include:

- Physically visit police station multiple times.
- Many police complaint management systems only store FIRs and NCRs, but not the original complaint. This can be a problem if a police officer refuses to file an FIR against an influential person, as the complainant will not have any proof that they filed a complaint.
- Centralized System: Single point of failure and hence more vulnerable to attack.
- Data Tampering: Storing FIR data in a local database can give the authority with the most power the ability to change important data without the approval of others.
- Police reluctance to register FIRs: The police are often reluctant to register FIRs, especially in cases where the accused is powerful or influential and fear reprisals from the accused or their supporters.
- Delays in registering FIRs: Even when the police agree to register an FIR, there are often delays in doing so. This can be frustrating for the victim, as it can delay the investigation and prosecution of the case.
- Inadequate investigation: Even when an FIR is registered, the police often do not conduct a thorough investigation. This can be due to a lack of resources, a lack of motivation, or a deliberate attempt to protect the accused.

Table I summarizes the differences between traditional systems and Blockchain systems. So, using a blockchain system, gives us the following benefits over traditional systems: Transparent, Secure, Immutable, and Decentralized.

III. Design of FIR-Chain

FIR-Chain uses blockchain technology to solve a major challenge in smart cities: ensuring the integrity of FIR data stored in a centralized database. By decentralizing control of FIR data among different entities, FIR-Chain can improve transparency and make it more difficult for data to be tampered with. The following are the important features of the proposed system:

- It uses a distributed blockchain ledger and smart contracts to provide tamper-proof and fraud-resistant FIR data integrity.
- The system collects the credentials of both the user and the administrator and stores them on the blockchain. This helps to prevent false FIR registrations by making it more difficult for people to impersonate or create fake accounts.
- It could also improve transparency and accountability in the police force.

As shown in Figure.1, the complainant first must register. Only after that can he use the FIR system. He must first fill out the standard FIR form through the proposed portal to report a complaint. Details like name, phone number, Aadhaar number, Police Station Id, and complaint details are to be entered. All the details of the complaint are to be stored on the blockchain. Documents related to the complaint can also be uploaded. These documents will be uploaded to Inter Planetary File System(IPFS), and their hash will be calculated. This hash and the complaint details are bundled together to form a transaction signed and sent to the blockchain. The transaction is then mined and stored in the blockchain. Users can track the status of registered complaints on their dashboard. It can be confirmed if FIR/Chargesheet for the complaint is registered or not. If, after certain days, there is no progress on the complaint, the complainant can go to a higher authority for it.

Once the complaint is registered, it is stored on the blockchain. The police personnel can access this complaint as per their police station Id. The police can then decide whether to file FIR depending on the complaint type and offense. FIR/NCR details are then stored on the blockchain. After filing the FIR/NCR, it is uploaded to IPFS also, which is available to the complainant, and its integrity is intact. Transactions made of details and documents are then stored on the blockchain.

Police Higher Authority can add police stations to the blockchain when required. For this purpose, a particular smart contract is created, which will be accessible only to a higher authority. Details of the police station, like address, station Id, Inspector in charge, etc., are added to the blockchain. Being a higher Authority, it can have various auditing rights and keep an eye on the working of police stations and their efficiency.

A. *Benefits of Proposed System*

- The complainants can easily file a complaint through a web application without going to a police station to register a complaint.
- No central database, i.e. No Single point of failure is used. Thus, the system is always available.
- By using IPFS, the system can ensure that FIRs, NCRs, and evidence are always available to the complainant and the police.
- The complainant can track the status of the filed complaint on its dashboard.

[4] https://ksp.karnataka.gov.in/new-page/cctns/en

[5] https://ncrb.gov.in/en/crime-and-criminal-tracking-network-systems-cctns

TABLE I
TRADITIONAL VS BLOCKCHAIN SYSTEMS

Feature	Traditional Systems	Blockchain systems
Centralization	Centralized	Decentralized
Security	Less Secure	More Secure
Transparency	Low	High
Scalability	Less scalable	More scalable
Cost	Less expensive to develop and maintain	More expensive to develop and maintain
Resistance to hacking	Less resistant	More resistant
Flexibility	More flexible	Less flexible
Consensus algorithm	No	Yes
Data storage	Centralized	Distributed
Data access	Private	Public
Data verification	Only authorized users can verify	Anyone can verify
Data Persistence	Non-persistence	Immutable
Performance	Fast	medium-fast

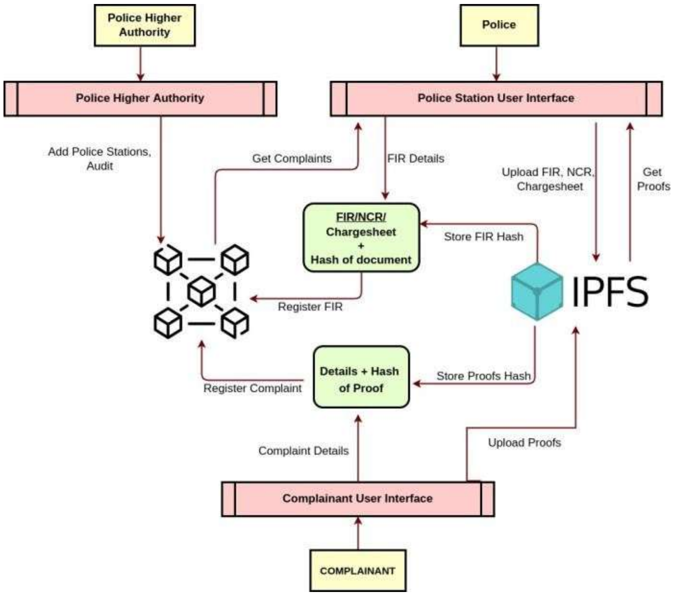

Fig. 1. Design of FIR-Chain

- Security: The blockchain ledger is tamper-proof and fraud-resistant, which makes it an ideal solution for storing sensitive data such as e-FIRs.
- Transparency: The blockchain ledger is transparent, auditable, and can be made publicly available, making it easy to track and verify FIR data.
- Accountability: The blockchain ledger can help to hold the police force accountable for their actions.

IV. IMPLEMENTATION OF FIR-CHAIN

FIR-Chain is implemented as web service using node server. The implementation can be divided into multiple modules.

- Complaint Registration Module
- Complaint Tracking Module
- Police Action Module
- Higher Authority Module

Each module is implemented using JavaScript and NodeJS server, and on the blockchain side, every module has a corresponding smart contract. The system leverages Go-Ethereum, Solidity, IPFS, and Django Web Server for its operation. The detailed working and implementation of each module are described below.

A. Complaint Registration module

A complainant submits complaint details through the web interface. Along with the complaint, files can be uploaded as supporting documents. These files are stored on **IPFS**, which generates a unique **content ID**. This ID is stored as part of the complaint details in the blockchain.

The registerComplaint.sol smart contract manages complaint registration. It includes the following structures:

- **struct Complaint:** Has fields for complaint details.
- **List comp:** An array storing all complaints.
- **mapping (string => string) stationIdToCompId:** Maps station IDs to complaint IDs.

- mapping (string => string) stationIdToCompId: To store the complaints IDs according to each stationId.

IThe addComplaint() API records the complaint details and the corresponding content ID. Once gave, the transaction is signed and sent to the blockchain, where miner nodes validate and commit it to the main chain.

Additionally, complaints are stored in Action.sol to track their status over time. This smart contract includes:

- **struct ComplaintProgress:** Stores complaint ID, timestamp, and progress updates.
- **mapping (string => uint256[]) cIdToActionIds:** Maps complaint IDs to action IDs.
- **mapping (uint256 => complaintProgress []) actionToComments:** Stores details of each action taken.

B. User Dashboard

The user dashboard allows complainants to:

- Register complaints.
- Track complaint status.
- View actions taken by police officers.

On the web server, the dashboard/username API retrieves all complaints linked to the user by calling getComplaintsForComplainant () from the smart contract. Complaint details are fetched from the blockchain and displayed on the dashboard.

Display complaint details and their status, the system uses the username/status/compliant API:

- getComplaintById () retrieves complaint details.
- The stored document is fetched from **IPFS** using the **content ID**.
- Status updates and actions are retrieved from the blockchain using getAllActions ().

The result, comprising **complaint details, uploaded files, and action updates**, is displayed on the user dashboard.

C. Police Dashboard and Action Module

The Police Dashboard allows officers to manage complaints. When a police officer logs in with a **station ID and password**, they are redirected to their respective station dashboard. The dashboard displays complaints assigned to their station.

To fetch complaints for a specific police station, the system uses the getComplaintsByStationId() API. This function:

- Retrieves complaints associated with the station from stationIdToCompId.
- Fetches complaint details and displays them on the dashboard.

Police officers can:

- View complaint status.
- Update progress (e.g., FIR/NCR registered, Under Investigation, Closed).
- Add comments and track action

The complaintId/TakeAction API allows officers to update complaint progress. Each action is recorded using:

- **New action ID**, stored in cIdToAllActionId.
- **Progress updates and comments**, saved in actionToComments.

If progress is updated to **FIR/NCR lodged**, the complaint is added to either **ListActionFir** or **ListActionNCR** accordingly.

V. Results and Analysis

A. Cost Analysis

Efficient smart contracts mean that it is executed at a higher speed and the operating cost is lower. To execute transactions on the blockchain, we require *gas*. The same contract should use the same amount of gas deployed on a blockchain [12]. Gas is the price incurred by using one unit of gas. To calculate the cost of an operation, we multiply the gas price by the amount used, as shown in equation 1.

*Total Cost = Gas Price * Amount of Gas Consumed* (1)

We have implemented and deployed four smart contracts. Table II shows the transaction costs in gas, its equivalent, and how those costs are converted into Rupees (|) for each function. On June 5, 2023, Ether's price was at |150,039.42 per ETH, the conversion value used in the table. As our blockchain is private, we set the gas price to 1 Gwei for easy calculation. The function caller covers this price if the system is deployed in the public blockchain.

B. Security Analysis

Using Ethereum as the foundation for our approach allows us to track all data flows, including user records, evidence files, and the updates posted by police personnel on the com- plaints/FIRs received. This data can be traced over time to provide full provenance. Ethereum also allows us to authenticate the addresses of stakeholders, ensuring that they are legitimate and cannot be impersonated. Our solution design ensures that each Ethereum address is associated with a single entity, preventing impersonation and Sybil attacks. Also, it makes sure that there are no malpractices involved in FIR registration like delaying/denying of FIR registration, modifying details of complaints without the complainant's approval, etc.

The system network is protected from cyberattacks by multiple layers of security.

Function Caller	Function Name	Transaction Cost (Gas)	Cost (Ether)	Cost (|)
User	addUser()	629,873	0.000629873	94.67
User	RegisterComplaint()	497,909	0.000497909	74.83
Police Station	UpdateProgress()	147,083	0.000147083	22.11
Police Station	TakeAction()	346,590	0.00034659	52.09
Higher Authority	AddPoliceStation()	170,597	0.000170597	25.64

The second layer is access control, which limits access to functions to registered identities and ensures that only specific entities can access functions that modify their data.

C. Comparison with existing solutions

We compared our solution with the existing solution [13] as shown in Table III. The table shows the superiority of FIR-Chain in terms of various aspects. This is because the system employs Blockchain technology, authentication mech- anisms, On-chain storage, data recoverability, Status update mechanisms, etc. Because of these, our solution becomes more robust, trustful, and user centered. Hence, we can say that FIR-Chain accomplishes all of the goals set by our initial design.

TABLE III
COMPARISON WITH EXISTING SOLUTION

Aspects	Khan et al. [13]	Our Solution
Privacy	Yes	Yes
Trustful	Partial	Yes
Immutability	Partial	Yes
Data Recovery	No	Yes
User Cenetered	Yes	Yes
Proof Uploading	No	Yes
Decentralized Storage	No	Yes
Detailed Status Check	No	Yes
Higher Authority Control	No	Yes
Decentralized Execution	Partial	Yes

VI. CONCLUSION

In this paper, we have proposed **FIR-Chain**, a blockchain-based system for secure and transparent FIR management. By leveraging **Node.js, React, Go-Ethereum, Solidity, and IPFS**, we have developed a decentralized platform that enhances the security, transparency, and efficiency of the complaint registration process. Create a local blockchain network. We created a web server

The integration of blockchain ensures that complaint records are **tamper-proof**, and IPFS provides a **secure storage mechanism** for uploaded documents. The system enables real-time tracking of complaint progress, fostering **accountability and trust** between the public and law enforcement agencies.

Despite its advantages, FIR-Chain faces challenges related to **scalability and transaction costs**, as blockchain networks require computational resources for mining and maintaining consensus. Future research will focus on **optimizing transaction processing times, reducing operational costs, and improving system scalability** to make FIR-Chain more practical for large-scale adoption.By conducting a **security assessment and cost-benefit analysis**, we have demonstrated that FIR-Chain is a **feasible and resilient solution** for modernizing FIR management. The implemented code has been made publicly available on **GitHub**, encouraging further

research and improvements in the domain of blockchain-based law enforcement systems.

REFERENCES

[1] "Code of Criminal Procedure-I," 2022, [Online; accessed 2022-12-9].

[2] "THE CODE OF CRIMINAL PROCEDURE, 1973," 2023, [Online; accessed 2023-06-12].

[3] "Status of Policing Report in 2018: A study of Performance and Perceptions," 2022, [Online; accessed 2022-07-20].

[4] A. Gupta and D. V. Jose, "A method to secure fir system using blockchain," vol. 8, no. 1, 2019, p. 4.

[5] M. A. Tasnim, A. A. Omar, M. S. Rahman, M. Bhuiyan, and Z. Alam, "Crab: Blockchain based criminal record management system," in *International conference on security, privacy and anonymity in computation, communication and storage*. Springer, 2018, pp. 294–303.

[6] K. Marmat and A. More, "E-fir using e-governance," *IJIRST*, vol. 3, 2016.

[7] N. D. Khan, C. Chrysostomou, and B. Nazir, "Smart fir: Securing e-fir data through blockchain within smart cities," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1–5.

[8] V. Hassija, A. Patel, and V. Chamola, "Police fir registration and tracking using consortium blockchain," in *Advances in Machine Learning and Computational Intelligence*. Springer, 2021, pp. 785–794.

[9] K. Tabassum, H. Shaiba, S. Shamrani, and S. Otaibi, "e-cops: An online crime reporting and management system for riyadh city," in *2018 1st International Conference on Computer Applications Information Security (ICCAIS)*, 2018, pp. 1–8.

[10] E. Nyaletey, R. M. Parizi, Q. Zhang, and K.-K. R. Choo, "Blockipfs - blockchain-enabled interplanetary file system for forensic and trusted data traceability," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 18–25.

[11] A. T. Dini, E. G. Abete, M. Colombo, J. Guevara, B. S. M. Hoffmann, and M. C. Abeledo, "Analysis of implementing blockchain technology to the argentinian criminal records information system," in *2018 Congreso Argentino de Ciencias de la Informa´tica y Desarrollos de Investigacio´n (CACIDI)*. IEEE, 2018, pp. 1–3.

[12] N. Ali, "Smart contract and transaction fee on ethereum," 04 2022.

[13] N. D. Khan, C. Chrysostomou, and B. Nazir, "Smart fir: securing e-fir data through blockchain within smart cities," in *2020 IEEE 91st vehicular technology conference (VTC2020-Spring)*. IEEE, 2020, pp.