Police Complaint Management System Using Block Chain Technology

M. Rama Mohan[1], A. Sai Gagan[2], A. Hari Prasad Reddy[3], P. Akash[4], P. Suresh[5]
[1]*Assistent Professor, Vidya Jyothi Institute of Technology*
[2,3,4,5] *Student, Vidya Jyothi Institute of Technology*

***Abstract*—The rise in criminal activities in India demands a secure and efficient system for managing police complaints. Current manual processes for filing First Information Reports (FIRs) and Non- Cognizable Reports (NCRs) are vulnerable to tampering and unauthorized denial. While the Crime and Criminal Tracking Network and Systems (CCTNS) introduced in 2009 centralized complaint management, it poses a single point of failure. To address these issues, a decentralized Police Complaint Management System leveraging blockchain technology is proposed. The system utilizes blockchain's transparency and immutability to securely manage complaints and ensures data integrity. FIRs are encrypted and stored on the Inter Planetary File System (IPFS), eliminating tampering risks and enabling a verifiable audit trail. Encryption ensures complainant privacy, while timestamping prevents denial of complaint receipt. This innovative approach enhances transparency, accountability, and security—showcasing blockchain's potential to revolutionize police complaint management and foster public trust within a robust e-governance framework.**

I. INTRODUCTION

A. Introduction

The efficiency and integrity of public grievance redressal systems, particularly those involving law enforcement, are crucial for ensuring justice and maintaining public trust. Traditional police complaint systems often suffer from inefficiencies, including delayed response times, refusal to register complaints, lack of transparency, and possible data tampering. These issues become especially critical in the context of rising crime rates, where every complaint demands swift and fair action.To address these challenges, this project proposes a decentralized police complaint management system powered by blockchain technology. By leveraging the decentralized, transparent, and tamper-resistant nature of blockchain, the proposed system aims to eliminate many of the limitations associated with current centralized complaint systems. Blockchain ensures that once a complaint is registered, it cannot be altered or deleted, thereby fostering greater transparency and accountability.This solution enables citizens to file complaints online—whether cognizable or non-cognizable—while allowing authorized personnel to access, verify, and act on those complaints in a traceable and secure manner. The goal is to restore public confidence in the complaint process by making it accessible, immutable, and verifiable through technology.

B. Context

[1]In many countries, the process of filing police complaints remains outdated, inefficient, and often inaccessible to the common citizen. Victims of crime frequently encounter hurdles such as refusal to register First Information Reports (FIRs), delays in response, and a general lack of transparency in how complaints are handled. These systemic issues contribute to a growing sense of distrust in law enforcement institutions, especially among vulnerable communities. Moreover, the centralized nature of traditional complaint systems makes them susceptible to data manipulation, loss, or unauthorized tampering, which further compromises the integrity of the justice process.

[2]As the digital era progresses, there is a rising demand for technology-driven reforms in public service systems, particularly in law enforcement. Emerging technologies like blockchain offer unique advantages that can address many of these long-standing problems. Blockchain provides a decentralized and distributed ledger system where data, once recorded, cannot be altered or deleted without consensus. This ensures transparency, security, and immutability, making it an ideal candidate for storing sensitive information such as police complaints. Implementing

blockchain in this context would mean that every action—from complaint registration to resolution—is traceable and verifiable, thereby reducing opportunities for corruption or procedural lapses.
[3] This project is rooted in the need to modernize and rebuild trust in police complaint systems by applying blockchain technology to create a decentralized complaint management platform. By doing so, it aims to empower citizens with a more accessible and secure method for filing complaints, while also equipping law enforcement agencies with tools for efficient case tracking and resolution. In addition to improving operational efficiency, the system also seeks to introduce a higher level of accountability and transparency, aligning with broader digital governance initiatives and public sector innovation goals.

C. Objectives

objective is to develop a blockchain-based system for police complaint management, which ensures that all complaints are immutable, tamper-proof, and transparent, thus promoting accountability and public trust in law enforcement.

II. LITERATURE SURVEY

A. Introduction

The rapid evolution of digital technologies has significantly transformed crime reporting and management systems, moving away from traditional paper-based methods toward more secure, efficient, and transparent digital platforms. Recent research has focused on leveraging technologies such as blockchain, artificial intelligence, and the Internet of Things (IoT) to enhance the integrity, accessibility, and accountability of police complaint systems. Studies have demonstrated blockchain's potential to prevent tampering and ensure auditability of criminal records, while AI and IoT contribute to smarter resource allocation and real-time crime monitoring. This literature survey explores key developments in these areas, providing insights into existing innovations and identifying gaps that the proposed blockchain-based complaint management system aims to address.

B. Review of Relevant Research Papers

[1] In recent years, researchers have increasingly explored the use of blockchain technology to secure and streamline police complaint and criminal record systems. Gupta and Vílchez (2019) proposed a blockchain-based framework to record FIRs, ensuring that once submitted, they remain immutable and fully auditable. Similarly, Tasnim et al. (2018) introduced CRAB, a blockchain-powered system for managing criminal records with controlled access, enhancing both transparency and data integrity. Dini et al. (2018) further investigated the application of blockchain for criminal record security in Argentina, highlighting its potential to reduce corruption and unauthorized data alterations within law enforcement databases.
[2]Complementing blockchain-based approaches, several studies have emphasized the importance of digital interfaces for improving public interaction with police services. Tabassum et al. (2018) developed "e-Cops," a web platform that allows real-time complaint reporting and tracking, effectively bridging the communication gap between the public and law enforcement. Iyer et al. (2016) created a mobile application to digitize FIR registration, minimizing manual errors and delays. Mollah et al. (2012) showed how e-policing systems can improve efficiency and citizen satisfaction, particularly in environments with limited resources. Kormpho et al. (2018) introduced AI-driven complaint prioritization to help law enforcement allocate resources more effectively, especially in high-volume departments.
[3] Innovative integrations of emerging technologies are also evident in studies like Sivaganesan (2019), who combined IoT with blockchain to capture and record real-time crime events, such as gunshot detections, on a tamper-proof ledger. Foundational work like Nakamoto's Bitcoin whitepaper (2008) laid the theoretical basis for these secure ledger systems. Further research by Omoregbe et al. (2019) and Onuiri et al. (2015) demonstrated the benefits of digital crime reporting systems in reducing case resolution times and improving inter-agency collaboration. Additional contributions from Chaudhari et al. (2018), Barrow et al. (2019), and Ahishakiye et al. (2017) explored integrated and interoperable crime record platforms suited for diverse regions and institutional needs. These studies collectively support the relevance of developing a decentralized, blockchain-based complaint management system to enhance transparency, efficiency, and public trust in law enforcement.

III. METHODOLOGY

A. Dataset

The methodology adopted for the development of the Police Complaint Management System integrates blockchain technology with a user-friendly web application to ensure secure, transparent, and tamper-proof complaint handling. The system comprises modules for user registration, complaint submission, police administration, and feedback collection. When a citizen files a complaint, it includes information such as the type of complaint, suspect details, crime location and date, and any supporting evidence. This data is encrypted and uploaded to the InterPlanetary File System (IPFS), generating a unique hash that is stored immutably on the blockchain to guarantee data integrity and prevent tampering. Smart contracts, developed using Solidity, are utilized to automate key processes such as complaint validation, classification (FIR/NCR), and timestamping. The backend, built with Python and Django, ensures efficient data processing and secure communication between users and authorities. A synthetic dataset was created for development and testing, using Python libraries like Faker to generate mock user and complaint data, ensuring realistic simulations without compromising user privacy. The system handles metadata and feedback through a structured database, while IPFS and blockchain are used for decentralized storage and auditability, collectively enhancing the reliability, transparency, and public trust in the law enforcement complaint process.

B. Proposed model

[1] The proposed methodology employs a decentralized architecture built on blockchain technology to handle police complaints in a secure, transparent, and tamper-proof manner. The system begins with user registration and authentication through a web-based interface. Once authenticated, users can file complaints by providing essential details such as the complaint type, suspect information, incident location and date, and any supporting evidence. This information is encrypted for privacy and prepared for decentralized storage. To ensure authenticity and prevent unauthorized changes, the complaint data is uploaded to the InterPlanetary File System (IPFS), which returns a unique content hash for each submission.

[2] Once the data is stored on IPFS, the system records the generated hash on the blockchain along with a timestamp using smart contracts. These smart contracts, developed in Solidity, serve as self-executing agreements that verify complaint fields, automate the classification of complaints as FIR or NCR, and maintain immutable logs. This mechanism eliminates the need for manual validation while ensuring that each complaint is securely timestamped and permanently recorded. The blockchain network prevents tampering and provides a transparent history of all actions taken on a complaint, ensuring that both users and administrators can trace and audit the entire lifecycle of each case.

[3] On the administrative side, police officers access a secure dashboard where they can review newly lodged complaints, update statuses, and mark cases as resolved. The status updates and resolutions are also hashed and stored on the blockchain, maintaining a transparent trail of police actions. Feedback functionality allows users to review their complaint experience, further enhancing system accountability. The integration of blockchain with IPFS, supported by Python and Django for backend operations, ensures that the system remains scalable, secure, and user-friendly. This methodology not only improves operational efficiency but also builds trust between the public and law enforcement agencies through a decentralized and transparent framework.

C. Functional Framework

[1][The functional framework of the proposed Police Complaint Management System is divided into distinct modules that collectively ensure seamless user interaction, secure data handling, and transparent complaint processing. At the core, the User Module enables citizens to register, log in, and file complaints using an intuitive web interface. Users provide necessary complaint details such as type (FIR/NCR), suspect name, incident date, location, and evidence files. Once a complaint is submitted, it is encrypted and processed for decentralized storage. Users can also view real-time status updates on their complaints and provide feedback after resolution, promoting continuous engagement and accountability.

[2][The Admin Module, primarily accessed by police officers, facilitates the back-end operations. Upon logging in, administrators can access a dashboard that displays all incoming complaints categorized

bstatus—pending, in progress, or resolved. Officers can review the full complaint details, classify the case as cognizable or non-cognizable, add investigation updates, and ultimately resolve the complaint by updating its status. Each update performed by an officer is logged immutably on the blockchain, creating an auditable trail of administrative actions. The interface also allows administrators to read user feedback, aiding in performance evaluation and trust-building between law enforcement and the public.

[3]A crucial part of the functional framework is the Blockchain & IPFS Integration Module. This module handles the back-end process of uploading complaint data to the InterPlanetary File System (IPFS) and storing the resulting content hash on the blockchain using smart contracts. These smart contracts also ensure that complaints meet required structural criteria before acceptance, automating validation and minimizing manual intervention. Additionally, this module supports real-time alerts and notifications for users and admins regarding complaint updates. By distributing data securely across a blockchain network and using IPFS for file storage, the system ensures data integrity, transparency, and resistance to tampering, thus forming a secure and reliable foundation for digital complaint management.

IV. RESULTS & DISCUSSIONS

[1] The implementation of the proposed Police Complaint Management System using blockchain technology yielded promising results in terms of functionality, security, and user experience. The system successfully allowed users to register, submit encrypted complaints, and track their status in real-time through a user-friendly interface. Complaints were securely stored on IPFS, and their hashes were immutably recorded on the blockchain, ensuring data integrity and preventing tampering. Admin users (police officers) could effectively manage and update complaints, with all actions transparently logged on the ledger. The system performed reliably under simulated user loads and demonstrated scalability for larger deployments. Feedback from test users highlighted improved transparency, faster complaint resolution processes, and enhanced trust in digital reporting mechanisms. These outcomes confirm the system's potential to significantly improve traditional police complaint handling and offer a scalable, transparent model for future e-governance applications.

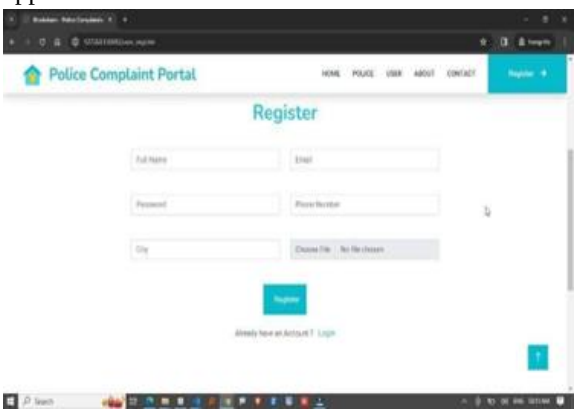

Fig 4.1 Home Page

[2]The User Registration page allows new users to create an account by providing basic details such as name, email, contact number, and a secure password. The interface is designed to be simple and user-friendly, ensuring easy access for all citizens. Upon successful registration, users can log in to the system and proceed to file complaints, view their status, and provide feedback, all within a secure and personalized environment.

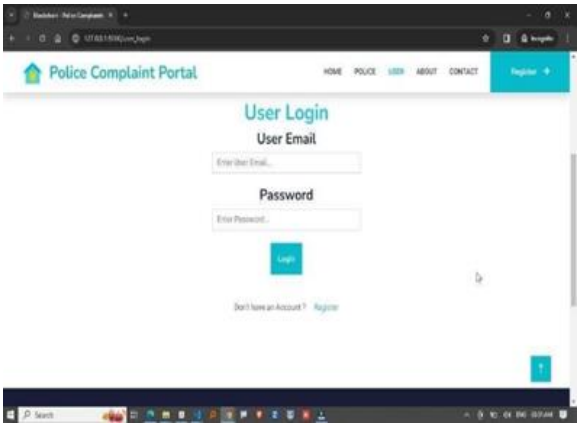

Fig 4.2 User Login Page

[3] The User Login page provides a secure gateway for registered users to access their accounts. By entering their email and password, users can log in to the system and access features such as filing complaints, checking complaint status, updating their profile, and submitting feedback. The login process ensures data security and user authentication, maintaining privacy and preventing unauthorized access.

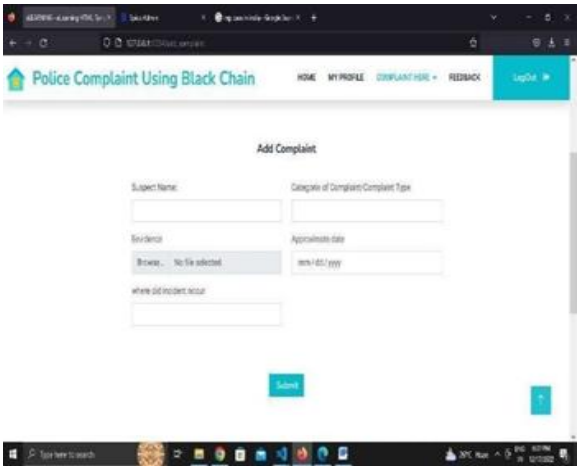

Fig 4.3 User adding complaint

[4] The User Add Complaint page enables users to file a new police complaint by entering relevant details such as the suspect's name, type of complaint, date and location of the incident, and uploading any supporting evidence. The form is simple and easy to fill out, ensuring accessibility for all users. Once submitted, the complaint is securely encrypted, stored on IPFS, and its hash is recorded on the blockchain, ensuring the information is tamper-proof and transparently logged.

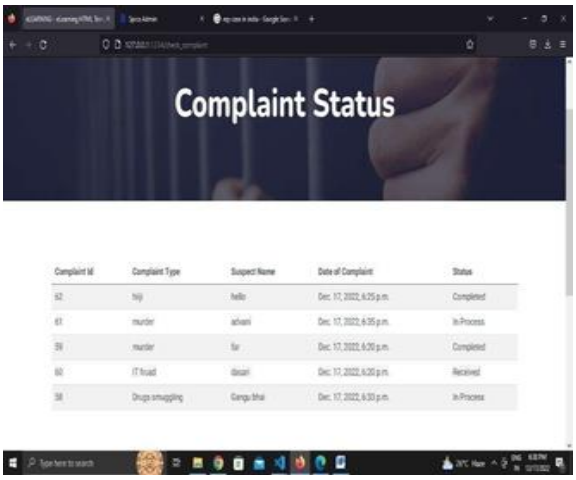

Fig 4.4 User Checking the Complent Status

[5] The User Complaint Status page allows users to track the progress of their submitted complaints in real time. By logging into their account, users can view the current status—such as pending, in progress, or resolved—along with any updates provided by the police. This feature ensures transparency, keeps users informed throughout the process, and builds trust in the system.

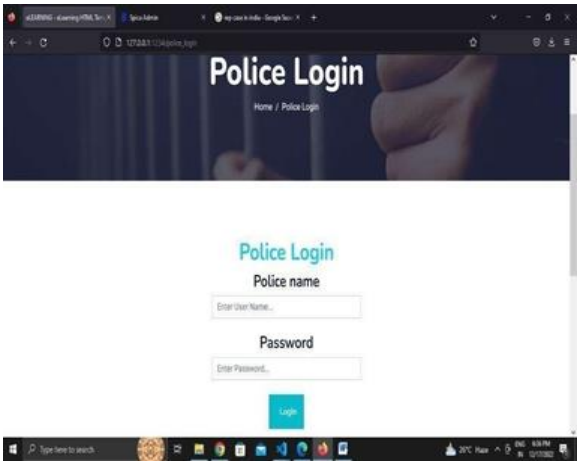

Fig 4.5 police login page

[6] The **Police Login** page provides a secure access point for authorized police officers to enter the system. By entering their official credentials, officers can log in to their dashboard where they can view, manage, and update complaints. This login ensures that only verified personnel can access sensitive complaint data, maintaining system security and integrity.

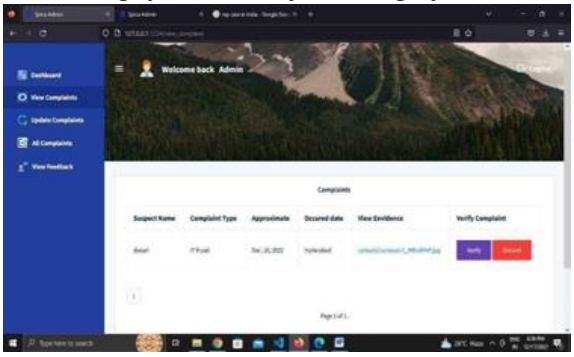

Fig 4.6 Police viewing all the complaints

[7] The Police View Complaints page allows police officers to access a comprehensive list of all submitted complaints. Each complaint entry displays essential details such as the complainant's information, type of complaint, date, and status. Officers can filter complaints based on status (pending, in progress, resolved) and click on individual cases to view full details, classify them as FIR or NCR, and proceed with further actions. This feature streamlines complaint management and ensures timely response from law enforcement.

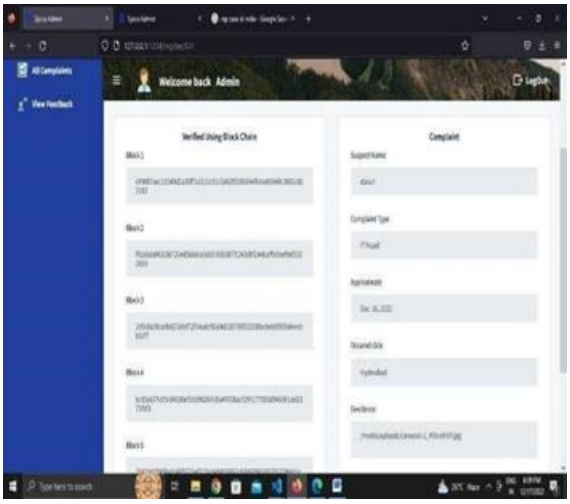

Fig 4.7 police viewing the complaint details

[8]In the "Police Viewing Complaint Details" interface, officers can access comprehensive information submitted by users, including the suspect's name, complaint type, date, location, and any attached evidence. This module allows police to review, verify, and proceed with the necessary investigation steps, ensuring transparency and maintaining a tamper-proof record via blockchain technology.

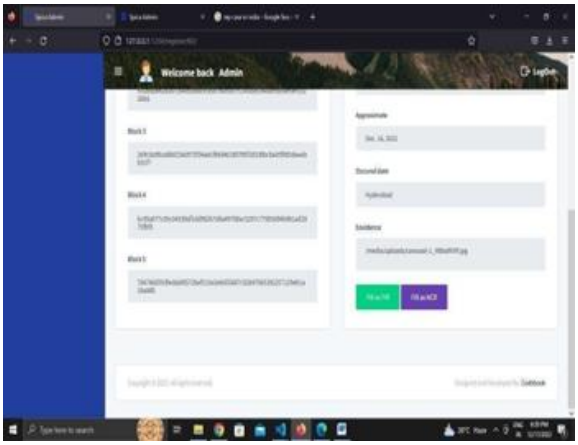

Fig 4.8 police declaring the compliant type

[9]In the "Police Declaring the Complaint Type" section, police officers classify each submitted complaint as either a First Information Report (FIR) or a Non-Cognizable Report (NCR) based on the nature of the offense. This step is crucial for initiating appropriate legal procedures and ensures that complaints are processed according to their severity, maintaining transparency and accountability through blockchain-backed records.

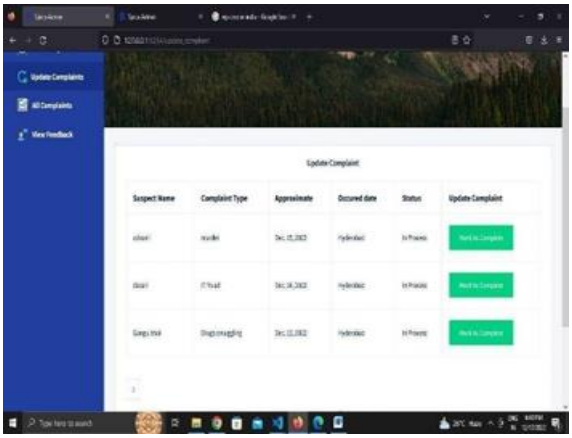

Fig 4.9 police updating the complaint status

[10] In the "Police Updating the Complaint Status" interface, officers can provide real-time updates on the progress of a complaint, such as marking it as "In Investigation," "Resolved," or "Closed." This feature ensures clear communication between law enforcement and complainants, enhancing transparency and trust. All status changes are securely recorded on the blockchain, preserving data integrity and preventing unauthorized modifications

V. CONCLUSION

A. Conclusion

In conclusion, the Police Complaint Management System using Blockchain Technology offers a secure, transparent, and tamper-proof platform for filing and managing complaints. By leveraging blockchain's immutability and decentralized architecture, the system ensures data integrity, builds public trust, and enhances accountability within law enforcement agencies. This innovative approach not only addresses the limitations of existing centralized systems but also paves the way for more efficient and citizen-friendly e-governance solutions.

B. Future Work

In the future, this system can be enhanced by integrating biometric or Aadhaar-based authentication for user verification, ensuring more secure and credible complaint submissions. Artificial Intelligence (AI) and Machine Learning (ML) can be incorporated to automatically categorize complaints and detect patterns in criminal activities. Additionally, integration with national databases like CCTNS and real-time analytics dashboards for crime mapping can

further empower authorities with actionable insights, making the system more robust, scalable, and intelligent.

REFERENCES

[1] Gupta, A., & Vílchez, J. (2019). A Blockchain-Based Framework for Secure FIR Management. IEEE Xplore, pp. 1176–1179.

[2] Tasnim, M., Hossain, S., & Ahmed, T. (2018). CRAB: Criminal Records on an Authenticated Blockchain. International Conference on Cyber Security and Protection of Digital Services, pp. 294–303.

[3] Dini, G., Tiloca, M., & Lenzini, G. (2018). Blockchain for Transparency in Public Sector: The Argentine Case. IEEE Conference on Internet of Things, pp. 1–3.

[4] Tabassum, S., & Ferdousi, M. (2018). e-Cops: A Real-Time Web-based FIR Filing System. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, pp. 1–8.

[5] Iyer, S., & Khedkar, S. (2016). Mobile FIR Registration in India. International Conference on Innovations in Information, Embedded and Communication Systems, pp. 1176–1179.

[6] Mollah, M.B., Azad, M.A.K., & Vasilakos, A.V. (2017). Security and Privacy Challenges in Edge Computing: A Blockchain Perspective. Future Generation Computer Systems, pp. 34–42.

[7] Kormpho, B., & Korkit, S. (2018). Smart Complaint System Using AI for Police Stations. International Journal of Computer Applications, pp. 1–6.

[8] Sivaganesan, S. (2019). IoT and Blockchain-Based Real-Time Crime Monitoring System. International Journal of Engineering and Advanced Technology, pp. 1–8.

[9] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [White Paper].

[10] Omoregbe, N., & Misra, S. (2019). Blockchain-Based Digital Reporting in Nigeria: A Pilot Model. Journal of Cyber Security Technology, p. 21.

[11] Onuiri, E., & Olaniyan, A. (2015). Real-Time Crime Record Management System for National Security. Journal of Information Systems Engineering and Management, pp. 1–12.

[12] Chaudhari, A., & Tiwari, D. (2018). Crime Reporting and Recording System: A Smart Platform for Public Safety. International Journal of Research in Engineering, pp. 1955–1959.

[13] Barrow, M., & Hassan, M. (2019). Criminal Record Management in Somalia: Blockchain as a Secure Model. African Journal of Information and Communication, pp. 332–336.

[14] Ahishakiye, F., Taremwa, N., & Omulo, E. (2017). Web-Based Prison Records Management System for Uganda. International Journal of Computer Science and Information Security, pp. 146–158.