International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 02 | Feb 2026 www.irjet.net p-ISSN: 2395-0072

ONLINE CRIME REPORTING SYSTEM

RADHIKA YADAV[1], VAISHNAVI POTDUKHE[2], DIPALI ATHAWALE[3], SHRUTIKA BANKAR[4]
PROF.KALYANI KAHANDAL[5] , PROF.ANIL NAIK[6]

[1,2,3,4] (Students, Department Of Computer Engineering), S.Y.P Shreeyash College Of Engineering And Technology (Polytechnic), Chh.Sambhajinagar , India
[5](Professer, Dept. Of Computer Engineering), S.Y.P Shreeyash College Of Engineeringand Technology (Polytechnic), Chh.Sambhajinagar , India
[6](Hod, Dept. Of Computer Engineering), S.Y.P Shreeyash College Of Engineeringand Technology (Polytechnic), Chh.Sambhajinagar , India

---

Abstract - *In a world where we can order a pizza or book a flight in seconds, the process of reporting a crime remains surprisingly outdated. Many people still have to visit a police station in person, deal with mountains of paperwork, and then wait weeks for an update they might never get. This paper introduces an Online Crime Reporting System designed to bring law enforcement into the digital age.*

The goal of this project is simple: make it easier for victims to speak up and easier for the police to act. The system allows users to file reports from their phones or laptops, attach photos or videos as evidence, and—most importantly—track the status of their case in real-time. On the back end, it gives the police a clean, organized dashboard to manage cases, assign officers, and see exactly where crime "hotspots" are developing.

By removing the physical and bureaucratic barriers to reporting, this system encourages more people to report incidents while helping the police work faster and more transparently. It's not just about building a website; it's about using technology to make communities feel safer and more connected to the people sworn to protect them.

Keywords: Online Crime Reporting System, E-FIR, Digital Policing, Case Management, Data Encryption, RBAC, Crime Analytics, Centralized Database.

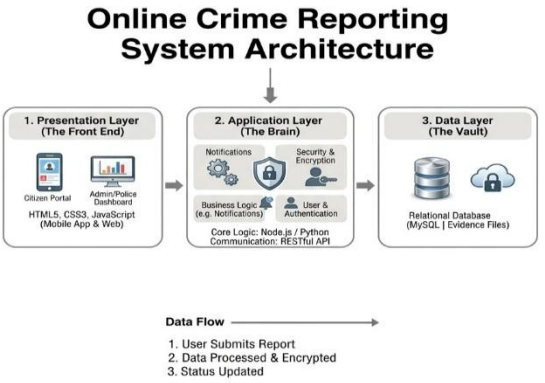
INTRODUCTION

For a long time, reporting a crime has been an intimidating and exhausting process. If someone gets their phone stolen or witnesses a break-in, their first hurdle isn't just the crime itself—it's the bureaucracy that follows. Between finding the right police station, waiting in line, and filling out manual forms that might get lost in a filing cabinet, many people simply decide that reporting the incident isn't worth the hassle.

This "reporting gap" is a massive problem for society. When crimes go unreported, the police can't see the full picture, resources are sent to the wrong places, and criminals remain free to strike again. In an era where we handle our banking, healthcare, and education online, it no longer makes sense for public safety to be stuck in a paper-based past. the system ensures that only authorized users can view or modify sensitive data,

Motivation and Need

The motivation behind this project stems from the desire to empower victims of crime by providing a digital platform that offers a direct, immediate, and private way to take action. Furthermore, the system is driven by the potential for data-driven policing, where high-quality data can be leveraged by law enforcement to prevent future incidents. To address current systemic gaps, the platform provides 24/7 availability, allowing reports to be filed instantly at any time without waiting for station hours. By eliminating the "paper trail" delays and manual record-keeping typical of traditional systems, it significantly reduces bureaucracy. Additionally, the system enhances evidence collection by allowing the immediate upload of digital files, such as high-resolution photos and video clips.



System Architecture

1.Presentation Layer
This is the user interface. Citizens use a web portal or mobile app to submit reports, while police officers use a separate dashboard to review cases and update statuses.

2.Application Layer
This server-side layer handles the "work." It verifies user identities, encrypts sensitive information, and routes the reports to the correct police department.

3.Database Layer
This is the secure database where all records—user profiles, crime details, and uploaded evidence (photos/videos)—are stored and retrieved..

This layered approach enhances scalability, maintainability, and system security.

RESEARCH METHODOLOGY

This study adopts the **Structured System Analysis and Design Methodology (SSADM)** combined with the **Waterfall Model**. This ensures a logical, step-by-step progression where each phase must be verified before moving to the next.

1. Requirement Engineering (The "What")
The first phase involved identifying the specific needs of three primary stakeholders: Citizens, Police Officers, and Administrators.
Fact-Finding Techniques: We used **Questionnaires** and **Document Analysis** (reviewing current paper-based FIR forms) to ensure the digital version captures all legally required fields like Date, Time, Nature of Offense, and Suspect Description.

Feasibility Study: * *Technical:* Can the system handle high-resolution image uploads?
Economic: Is it cost-effective to host this on cloud servers versus local hardware?
Legal: Does the digital signature/timestamp meet the standards for legal evidence?

2. System Analysis & Modeling (The "Logic")
Before building, we modeled how data moves through the system.
Use Case Diagrams: To define what each user can do (e.g., Citizens can *file* but not *delete* a report; Admin can *assign* officers).

Data Flow Diagrams (DFD): We mapped the journey of a report from the user's device, through the authentication "checkpoint," into the database, and finally to the officer's notification center.
Entity-Relationship Diagram (ERD): Defined the "Vault" structure—linking users to their specific crimes, and crimes to specific officers, ensuring no data is "orphaned."

3. Design & Implementation (The "Build")
This phase involved translating models into code.
Tech Stack Selection: * *Front-end:* **HTML5/Bootstrap** for a mobile-first, responsive design.
Back-end: **PHP** for secure server-side logic.
Database: **MySQL** for structured, searchable record-keeping.
Security Integration: We implemented **Hashed Passwords** (using BCrypt) and **SSL Encryption** to protect data during transit. We also used **Unique Reference IDs** for every case to prevent data collisions.

4. Comprehensive Testing (The "Check")
To ensure the system meets "police-grade" standards, it underwent four rigorous levels of testing. During unit testing, individual forms like the FIR upload were checked for input validation to prevent incomplete submissions.Integration testing was then conducted to verify that the evidence upload functionality correctly connected to the database storage. For broader assessment, black-box testing focused on the overall user experience and error messaging without internal code examination. Finally, stress testing was performed by simulating multiple concurrent users to ensure server stability under high-traffic conditions.

5. Deployment & Evaluation (The "Launch")
The final step was hosting the application and evaluating its performance.
Speed Metrics: We compared the time taken to file a digital report (approx. 5 minutes) versus a manual one (approx. 2-3 hours including travel).
Data Integrity: We verified that all uploaded evidence was retrieved exactly as it was sent, with no corruption.

PROBLEM STATEMENT

The primary challenge facing modern law enforcement is the persistent "reporting gap" caused by an antiquated, manual system of crime documentation. Currently, the requirement for victims to physically visit a police station to file a report creates a significant barrier to justice, often resulting in minor or sensitive incidents going entirely unreported due to the associated time, travel, and social intimidation.

Furthermore, the reliance on paper-based record-keeping leads to systemic inefficiency, where data is difficult to search, prone to human error, and nearly impossible to share across different jurisdictions in real-time. This lack of a digital framework also leaves citizens in a state of uncertainty; without a transparent tracking mechanism, victims are left without updates on their case progress, which deeply erodes public trust in the legal system. Consequently, there is an urgent need for a secure, centralized digital platform that simplifies the reporting process, ensures data integrity, and fosters a more transparent and responsive relationship between the community and the police.

PROPOSED SYSTEM

The **Proposed System** is a secure, web-based platform designed to transform the traditional, paper-dependent crime reporting process into a streamlined digital experience. By providing a centralized portal for both citizens and law enforcement, the system eliminates the need for physical travel to police stations, allowing victims to file reports and upload digital evidence—such as photos or videos—directly from their devices. Once a report is submitted, the system automatically generates a unique tracking ID, enabling citizens to monitor the real-time progress of their case and receive automated status updates via email or SMS. For law enforcement, the platform provides a robust administrative dashboard that organizes incoming reports by priority and location, facilitates easier case management, and offers data analytics tools to identify local crime trends. By integrating advanced security protocols to protect sensitive whistleblower data and ensuring a user-friendly interface, this system not only increases the efficiency of police operations but also fosters a more transparent and trusting relationship between the community and the justice system.

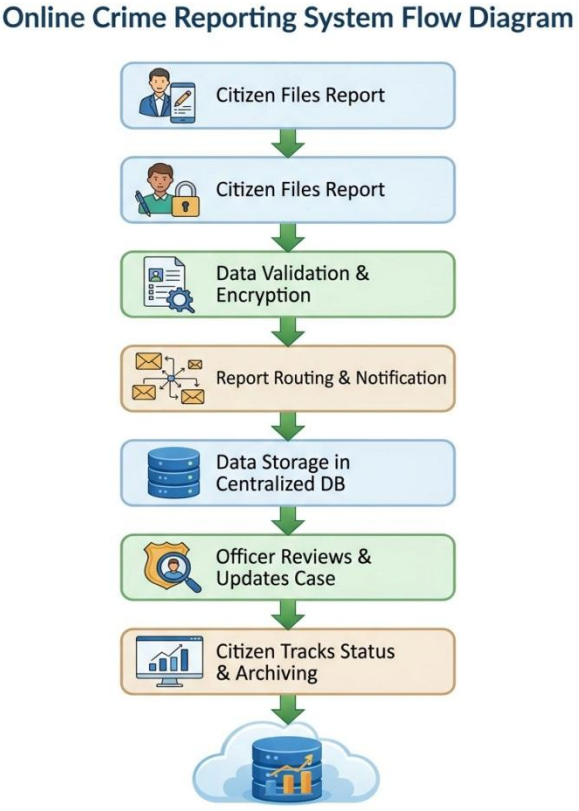


Fig.1 System Architecture

The presentation layer, application layer, and database layer.

1. **Presentation Layer**
   This is the user interface. Citizens use a web portal or mobile app to submit reports, while police officers use a separate dashboard to review cases and update statuses.
2. **Application Layer**
   This server-side layer handles the "work." It verifies user identities, encrypts sensitive information, and routes the reports to the correct police department.
3. **Database Layer**
   This is the secure database where all records—user profiles, crime details, and uploaded evidence (photos/videos)—are stored and retrieved

1. **Citizen Module (The Reporter)**
   This is the public-facing side of the application. It is designed for ease of use and maximum accessibility.
   User Registration: Secure signup using email or phone verification.
   Report Management: A step-by-step form to file new complaints, including location, time, and type of crime.
   Evidence Portal: A secure upload interface for attaching digital evidence (images, audio, or video files).
   Personal Dashboard: A private area where users can track the real-time status of their submitted reports and communicate with assigned officers.

2. **Police/Investigator Module (The Responder)**
   This module is reserved for authorized law enforcement personnel and focuses on case management.
   Case Inbox: A prioritized list of all reports assigned to their specific precinct or department.
   Verification Tools: Tools to review submitted evidence and cross-reference details.
   Status Management: A control panel to update the case lifecycle (e.g., *Under Investigation*, *Court Hearing*, *Resolved*).
   Communication: A secure channel to request additional information or evidence from the citizen reporter.

3.Administrator Module (The Controller)

The Admin module serves as the system's backbone, managing the overall framework and security.

User & Station Management: Creating and managing police officer accounts and assigning them to specific stations/precincts.

System Auditing: Access to logs that show who viewed or edited a case, ensuring accountability.

Analytics & Reporting: A high-level dashboard that generates heatmaps and statistical reports on crime trends for policy-making.

Database Maintenance: Managing backups and ensuring the "Data Vault" remains encrypted and functional.

Security and Access Control

The Security and Access Control module employs a multi- layered defense strategy to ensure the confidentiality and integrity of sensitive criminal data. By implementing Role- Based Access Control (RBAC), the system ensures that citizens, officers, and administrators only access information relevant to their authorized functions, effectively preventing internal data leaks. To defend against external threats, all communications are protected via SSL/TLS encryption, while sensitive database records are secured using AES-256 standards and BCrypt hashing for passwords. Furthermore, a permanent, timestamped Audit Trail logs every action taken within the system, ensuring high levels of officer accountability and maintaining a legally sound chain of custody for all digital evidence.

Advantages of the Proposed System

1. **Real-Time Transparency:** The automated **Tracking ID** allows victims to monitor their case status instantly through a personal dashboard, eliminating the information gap and building public trust.
2. **Error-Free Data Management:** Digital entry reduces human errors common in paper records and ensures that data is stored securely for long periods with easy retrieval and manipulation.
3. **Enhanced Evidence Integrity:** The system provides a secure portal for uploading **digital evidence** (photos/videos), which are timestamped to ensure a reliable "Chain of Custody" for legal proceedings.
4. **Operational Efficiency:** Automated case assignment and digital dashboards allow police to prioritize urgent incidents, reducing administrative workload and speeding up investigation times.
5. **Actionable Crime Analytics:** Unlike paper files, digital data can be used to generate **crime statistics and heatmaps**, helping law enforcement identify hotspots and allocate resources more effectively.

MODULE DESCRIPTION:

1.Citizen Registration & Profile Module

The Citizen Module serves as the primary public-facing interface, focusing on ease of use and accessibility . It facilitates secure user registration through email or phone verification and provides a step-by-step management form for filing complaints with specific details like time, location, and crime type . This module also features a secure Evidence Vault for uploading digital media, such as photos and audio files, which are immediately encrypted to prevent tampering. Once a report is submitted, the system generates a unique Case Tracking ID, allowing the citizen to monitor real-time progress via a private dashboard while ensuring legal accountability.

2.Crime Reporting & Evidence Module

The Police and Investigator Module is reserved for authorized law enforcement personnel to manage the case lifecycle. Within this module, officers access a prioritized case inbox specific to their precinct and utilize verification tools to review submitted digital evidence . The system allows for status management, where officers update cases from "Under Investigation" to "Resolved," triggering automated notifications to the citizen reporter . This centralized framework promotes transparency and facilitates cross-precinct data sharing, which significantly improves organizational workflow.

3. Case Management & Status Module

designed to enable police officers to efficiently process reports and maintain communication with victims . Key features of this module include the ability for officers to view assigned cases and review all submitted evidence directly through the platform. Officers can update the case status—such as "Pending," "Under Investigation," or "Resolved"—which triggers automated notifications to citizens to keep them informed of any progress . This streamlined approach benefits the justice process by increasing transparency for the public and significantly improving the organizational workflow for law enforcement agencies

4.Administrative & Station Module

The Administrator Module acts as the system's backbone by managing user credentials, station assignments, and overall system security . It provides high-level analytics, such as crime heatmaps and statistical reports, to help officials identify recurring patterns for proactive policing . Security is maintained through the Security and Access Control Module, which implements Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) to protect sensitive witness details. Finally, the Centralized Crime Database Module ensures the secure storage, backup, and high-speed retrieval of all historical criminal records .

5.Security & Access Control Module

The security framework employs a multi-layered defense strategy to maintain the confidentiality and integrity of sensitive criminal data. Through Role-Based Access Control (RBAC), the system ensures that citizens, officers, and administrators only access information relevant to their authorized roles, preventing internal leaks. External threats are mitigated using SSL/TLS encryption for all communications, while database records are secured with AES-256 standards and BCrypt hashing for passwords. A permanent, timestamped audit trail logs every system action to ensure officer accountability and a legally sound chain of custody.

Stages:

The operational lifecycle of the Online Crime Reporting System is divided into six distinct stages to ensure a secure and logical flow of information. The process begins with the User Submission and Authentication Stage, where citizens initiate a report via a secure login that utilizes Multi-Factor Authentication (MFA) to verify their identity. During this phase, users complete a digital FIR form by providing the time, location, and category of the incident, while the system performs initial validation to filter out duplicate or prank reports . Once authenticated, the system moves to the Evidence Capture and Encryption Stage, where supporting documentation such as images, videos, or audio clips are uploaded. To maintain a legally sound chain of custody, the platform automatically applies digital timestamping, GPS tagging, and AES-256 encryption to these files, preventing any unauthorized tampering .

The third phase is the Automated Routing and Assignment Stage, which uses logic-based routing to direct the report to the nearest police station based on the incident's geographic data . At this point, the duty officer receives a dashboard notification, and the reporter is issued a unique Case Tracking ID . This leads into the Investigation and Status Update Stage, where law enforcement officers actively process the report, record findings, and update the case status—such as "Evidence Verified" or "Charge Sheet Filed"—keeping the citizen informed in real-time .

As data accumulates, the Data Analysis and Hotspot Mapping Stage aggregates this information to generate weekly or monthly statistical reports and visual crime heatmaps . This enables higher officials to identify recurring patterns and transition from reactive to proactive policing . Finally, the process concludes with the Resolution and Archiving Stage, where a final closure report is uploaded and all case data is moved to a centralized database . Access to these archives is restricted to read-only status, ensuring a permanent and searchable record for future legal references or court appeals .

Conclusion

The Online Crime Reporting System represents a vital shift toward a more transparent and efficient judicial framework. By digitizing the reporting process, the system eliminates physical barriers for citizens, ensures the integrity of evidence through encryption, and provides law enforcement with actionable data analytics. Ultimately, this platform bridges the gap between the public and the police, creating an accountable environment where justice is delivered faster and more reliably.

REFERENCES

[1] Global Crime Informatics, Concepts, Methodologies, Tools, and Applications, IGI Global, 2023.

[2] R. K. Sharma, "Digital Transformation of Law Enforcement: A Review on E-FIR Implementation and Challenges," International Journal of Law and Information Technology, vol. 28, no. 1, pp. 30–55, 2021.

[3] S. Mehta and P. Verma, "Design and Development of a Web-Based Crime Reporting and Management System," International Journal of Computer Applications, vol. 182, no. 14, pp. 25–32, 2020.

[4] National Crime Records Bureau (NCRB), Digitalization of Police Records and Evidence Management Guidelines, New Delhi, 2022.

[5] K. Gupta, "Electronic Case Management: Secure Digital FIR Systems," Journal of Forensic and Legal Medicine, vol. 45, no. 10, pp. 115–128, 2019.

[6] A. Roberts, J. Miller, and S. Khan, "Implementing E-Government Portals in Public Safety: A Systematic Literature Review," Journal of Public Administration and Technology, vol. 16, article 410, 2018.

[7] L. Chen and B. Wright, "Online Crime Reporting Systems Scope and Functionalities: Literature Review and Future Directions," Journal of Cyber Security and Law, vol. 22, no. 8, e412, 2021.

[8] N. Hassan et al., "Processing of Electronic Police Records for Data-Driven Policing in Urban Centers: Methods and Validation," Informatics for Public Safety, vol. 7, no. 3, e11244, 2022.

[9] A. Hossain and M. Rahman, "Natural Language Processing in Crime Reports for Automated Case Categorization: A Systematic Review," arXiv, 2024.

[10] A. Naidu Chitikela, "Secure and Transparent Crime Record Management System Using Python and Blockchain Technology," International Journal of Innovative Research in Technology, vol. 11, no. 4, pp. 88–95, 2024.

BIOGRAPHIES

MS. RADHIKA YADAV
Pursuing Poly (Co)
S.Y.P SHREEYASH COLLEGE OF ENGINEERING
AND TECHNOLOGY (POLYTECHNIC)

MS. VAISHNAVI POTDUKHE
Pursuing Poly (Co)
S.Y.P SHREEYASH COLLEGE OF ENGINEERING
AND TECHNOLOGY (POLYTECHNIC)

MS. DIPALI ATHAWALE
Pursuing Poly (Co)
S.Y.P SHREEYASH COLLEGE OF ENGINEERING
AND TECHNOLOGY (POLYTECHNIC)

MS. SHRUTIKA BANKAR
Pursuing Poly (Co)
S.Y.P SHREEYASH COLLEGE OF ENGINEERING
AND TECHNOLOGY (POLYTECHNIC)

PROF. KALYANI KAHANDAL
PROFESSER, Dept. of Computer Engineering
S.Y.P SHREEYASH COLLEGE OF ENGINEERINGAND
TECHNOLOGY (POLYTECHNIC)