STM JOURNALS

Journal of
Advanced Database
Management & Systems

ISSN: 2393-8730
Volume 12, Issue 3, 2025
September–December
DOI (Journal): 10.37591/JoADMS

https://journals.stmjournals.com/joadms

Review JoADMS

A MERN-Based Crime Management System: Enhancing Crime Reporting and Law Enforcement Collaboration

Bhanu Verma[1,*], Monika Nagar[2], Laiba Saifi[3], Khushi Bhatia[3], Devanshi Vishwakarma[3]

Abstract

In the modern digital age, efficient crime management is essential for safeguarding the public and upholding law and order. This project introduces the development of a Crime Management System (CMS) built with the MERN stack (MongoDB, Express.js, React, Node.js) to streamline crime reporting, monitoring, and coordination among law enforcement agencies. The CMS is designed to streamline the processes of crime reporting, record management, and data analysis, addressing inefficiencies in traditional manual systems. The system enables authorized users, such as police officers and administrators, to record and manage crime-related data, including case details, suspect profiles, and victim information. Key functionalities include user authentication, secure data entry, efficient retrieval mechanisms, and comprehensive reporting. The database schema is meticulously designed to handle relational data with entities such as crimes, cases, users, and locations, ensuring data consistency and integrity. The Crime Management System project is designed to offer a reliable and effective solution for storing, accessing, and handling crime-related information. By organizing crime data effectively, law enforcement agencies can gain insights, track patterns, and enhance crime prevention strategies. This study discusses the design, functionality, and impact of this Crime Management System in supporting crime data handling and analysis.

Keywords: Crime management system, data handling, data storage, system functionality, digital crime reporting

INTRODUCTION

Crime is a critical issue that affects societies worldwide. Effective crime management is essential for ensuring public safety, maintaining law and order, and improving the efficiency of law enforcement agencies. However, traditional crime management systems often suffer from delays, lack of transparency, manual inefficiencies, and limited accessibility. To overcome these issues, we introduce a Crime Management System (CMS), a web-based platform developed with the MERN stack (MongoDB, Express.js, React.js, and Node.js). The system serves as a unified digital solution for reporting, monitoring, and managing criminal activities. Citizens can report crimes online, law enforcement can investigate and update case statuses, and administrators can analyze crime trends using advanced data visualization tools.

CMS is an application that provides facility for storing data related to crimes and criminals online. The application maintains detailed records of criminals, cases, and their histories, all organized within a centralized database. Unlike conventional

***Author for Correspondence**
Bhanu Verma
E-mail: bhanu.verma@imsec.ac.in

[1]Assistant Professor, Department of Information Technology, IMS Engineering College, Ghaziabad, Uttar Pradesh, India
[2]Assistant Professor, Department of Computer Science, IMS Engineering College, Ghaziabad, Uttar Pradesh, India
[3]Student, Department of Computer Science, IMS Engineering College, Ghaziabad, Uttar Pradesh, India

Received Date: September 08, 2025
Accepted Date: September 12, 2025
Published Date: October 15, 2025

Citation: Bhanu Verma, Monika Nagar, Laiba Saifi, Khushi Bhatia, Devanshi Vishwakarma. A MERN-Based Crime Management System: Enhancing Crime Reporting and Law Enforcement Collaboration. Journal of Advanced Database Management & Systems. 2025; 12(3): 40–52p.

methods of managing crime-related data, such as paper files or obsolete software systems, which are often error-prone, inefficient, and vulnerable to security threats, this approach ensures accuracy, efficiency, and better data protection. This hampers the ability of law enforcement officers to efficiently manage case information, track the progress of investigations, and retrieve critical data when needed. Furthermore, the lack of a centralized system makes it difficult to analyze crime trends, which is essential for strategic planning and resource allocation.

This project primarily aims to assist the police in maintaining and managing all case-related information within a centralized database. With this software, police no longer need to maintain records manually, as all data is securely stored in a centralized database. Many crimes often go unreported, so, this application simplifies the crime reporting process. The system incorporates security protocols to guarantee access is restricted to authorized users only, with the objective of delivering a dependable platform for law enforcement agencies. Additionally, this application reduces manual workload by offering an automated, secure, and real-time solution. It enhances communication between citizens and authorities, enabling faster crime reporting, efficient case tracking, and data-driven decision-making.

The application contains data ranging from details of criminals to the crime they are involved in. A separate class for officers which contains their ranks and the roles officers are assigned. The system simplifies the process of submitting reports, ensuring that every crime is documented and none go unreported. The main idea of application is welfare of public and easy accessibility of these records to general police without much hassle. To overcome these challenges, this project introduces the development of a Crime Management System (CMS). The CMS serves as a complete solution aimed at streamlining and automating crime reporting and case management processes and data analysis. By integrating technology into the workflow of law enforcement agencies, the system aims to streamline operations, reduce errors, and enhance decision-making capabilities.

The CMS facilitates the digital recording of crime-related data, including details of reported crimes, suspects, victims, and case statuses. The platform includes advanced search features that enable users to access information using different filters, such as type of crime, date, or location. Additionally, it provides robust reporting tools to generate detailed reports and analyze crime trends over time, aiding strategic planning and resource allocation.

The system includes the following key features:

For Citizens

- User Registration and Authentication (using JWT-based authentication).
- Crime Reporting Portal (submit details, upload evidence, and track progress).
- Real-time Status Updates (notifications on case progress).
- Secure Communication (chat or message authorities securely).

For Law Enforcement Officers

- Case Assignment and Tracking (assign officers to cases and monitor progress).
- Document and Evidence Management (upload case-related documents, images, and videos).
- Crime Analytics and Reports (generate insights, trends, and statistics).
- Role-based Access Control (secure access based on user roles).

For Administrators

- User and Role Management (manage access for police, citizens, and admins).
- Crime Trend Analysis (visual dashboards for monitoring crime rates).
- System Monitoring and Logs (track user activity for security and auditing).

OBJECTIVE

The objective of the Crime Management System built using the MERN (MongoDB, Express.js, React, Node.js) stack is to create a secure, efficient, and user-friendly platform for managing and reporting crimes. The system aims to:

1. *Streamline Crime Reporting:* Allow citizens to report crimes online easily and securely.
2. *Centralized Crime Database:* Store and manage crime records efficiently using MongoDB for quick access and retrieval.
3. *Real-time Status Updates:* Enable users to track the progress of their reported cases.
4. *Role-Based Access:* Ensure secure access for citizens, police officers, and administrators with proper authentication and authorization.
5. *Data Analysis and Visualization:* Provide crime statistics, heatmaps, and reports to help authorities analyze crime trends.
6. *Evidence and Document Management:* Allow secure upload and storage of case-related documents, images, and videos.
7. *Efficient Case Handling:* Help law enforcement assign, track, and update cases in real-time.
8. *Secure Communication:* Facilitate communication between citizens and law enforcement through a secure messaging system.
9. *User Authentication:* Implement JWT-based authentication for secure login and role management.
10. *Mobile Responsiveness:* Ensure the system is accessible on desktops, tablets, and smartphones.

TECHNOLOGY USED

Technology used for building the application is MERN stack. The MERN stack was chosen for its efficiency, scalability, and flexibility:

- *MongoDB:* A NoSQL database to store crime records, user data, and evidence securely.
- *Express.js:* A lightweight backend framework for handling API requests and managing authentication.
- *React.js:* A dynamic front-end framework to provide an interactive and user-friendly interface.
- *Node.js:* A scalable runtime environment to handle backend logic and server-side processing.

Let us understand the MERN stack in detail shown in Figure 1.

MongoDB (Database NoSQL)

MongoDB is a NoSQL, document-oriented database built to handle and manage application data. In contrast to relational databases such as MySQL or PostgreSQL that rely on tables and rows, MongoDB stores information in JSON-like documents (BSON format), offering enhanced scalability and flexibility.

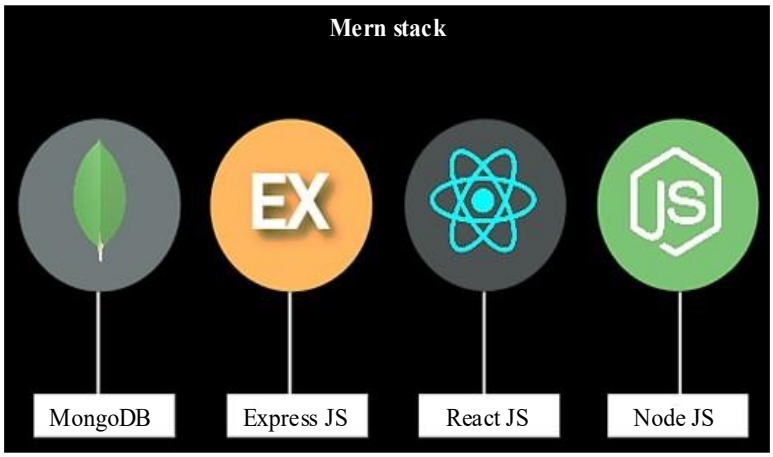

Figure 1. Technologies in MERN.

Key Features of MongoDB

- *Schema-less Database:* You can store different types of data structures in the same collection.
- *Scalability:* Supports horizontal scaling (sharding) for handling large amounts of data.
- *Fast Performance:* Uses indexing and in-memory storage for faster data retrieval.
- *JSON-based Documents:* Data is stored in a format similar to JSON, making it easy to work with JavaScript applications.

MongoDB is used in the Crime Management System to store user details, crime records, case status, and officer assignments securely.

Express.js (Backend Framework)

Express.js is a lightweight and fast Node.js framework that simplifies backend development by handling server-side logic, routing, and API requests efficiently.

Key Features of Express.js

- *Minimalistic and Fast:* Provides a simple and lightweight structure for backend development.
- *Middleware Support:* Allows processing of requests (authentication, logging, etc.).
- *RESTful APIs:* Makes it easy to create API endpoints for communication between frontend and backend.
- *Seamless Integration:* Works perfectly with MongoDB and React.js in the MERN stack.

In the Crime Management System, Express.js is used for handling API requests, managing user authentication, and performing CRUD (Create, Read, Update, Delete) operations on the database.

React.js (Frontend Framework)

React.js is a JavaScript library designed for developing interactive and dynamic user interfaces. It enables developers to build reusable UI components, enhancing the speed, efficiency, and scalability of web applications.

Key Features of React.js

- *Component-Based Design:* The user interface is structured into reusable and modular components.
- *Virtual DOM:* Improves efficiency by re-rendering only the modified elements of the interface.
- *Unidirectional Data Flow:* Ensures stronger control and predictability in how data moves across components.
- *Hooks and State Handling:* Utilizes React Hooks like *useState* and *useEffect* for streamlined and effective state management.

In the Crime Management System, React.js is used for creating the user interface, allowing citizens to report crimes, view case statuses, and enabling police officers to manage cases interactively.

Node.js (Runtime Environment)

Node.js is a runtime environment for JavaScript that operates on the server side, allowing developers to run JavaScript code beyond the browser. Powered by Google Chrome's V8 engine, it delivers high speed and efficiency, making it ideal for managing real-time applications.

Key Features of Node.js

- *Asynchronous and Event-Driven:* Handles multiple requests without blocking the system.
- *Single Programming Language:* Uses JavaScript for both frontend and backend development.
- *Fast and Scalable:* Non-blocking I/O model allows handling multiple requests simultaneously.
- *NPM (Node Package Manager):* Offers thousands of open-source libraries for rapid development.

WHY MERN STACK?

The MERN stack is a modern, versatile, and efficient technology stack that empowers developers to build scalable, high-performance, and user-friendly web applications. In the Crime Management System, it facilitates smooth interaction between users and law enforcement, enables effective case tracking, and ensures secure data handling.

How Mern Stack Works Together

1. *Frontend (React.js):* The user interacts with the web application through a dynamic UI built with React as shown in Figure 2.
2. *Backend (Express.js + Node.js):* The Express server handles requests from the frontend and processes business logic.
3. *Database (MongoDB):* Stores and retrieves data related to crime reports, users, and cases.
4. *API Communication:* React makes API calls to Express.js, which interacts with MongoDB to fetch or store data.

LITERATURE REVIEW

A Crime Management System is an essential tool in modern law enforcement, enabling the digitization of crime reporting, tracking, and investigation processes. To develop an efficient and scalable system, it is necessary to examine existing literature, technological advancements, and previous research on crime management and digital policing.

This literature review explores traditional crime reporting systems, modern crime management technologies, and the role of the MERN stack in web-based applications. There are several systems related to our project that have been proposed earlier. Some of them are described below. Now the aim was to make our project standout from these earlier proposed systems. These earlier systems have few limitations and difference with our system with technologies.

"Crime Detection and Criminal identification in India Using Data Mining Techniques" by Tayal et al. [1]

This paper presents a proposed methodology for designing and implementing a crime detection and criminal identification system for Indian cities using data mining techniques [1]. The system is structured into six key modules: data extraction, data preprocessing, clustering, Google Maps integration, classification, and final implementation. This approach aims to enhance societal safety by assisting law enforcement agencies in identifying criminals and detecting crimes, ultimately contributing to a reduction in crime rates.

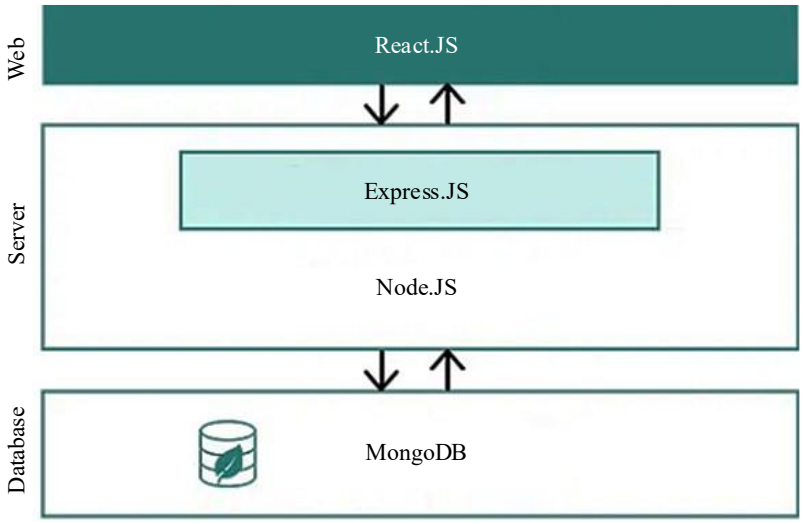

Figure 2. Working of MERN.

“Crime Analysis and Prediction” by Sathyadevan et al. [2]

Crime analysis and prevention involve a structured approach to identifying and examining crime patterns and trends [2]. This system can predict areas with a high likelihood of criminal activities and visualize regions prone to crime. With the rise of computerized systems, crime data analysts assist law enforcement agencies in accelerating the crime-solving process. By leveraging data mining techniques, valuable and previously undiscovered insights can be extracted from unstructured data. This approach bridges computer science and criminal justice to develop a data mining methodology that enhances crime-solving efficiency. Instead of emphasizing factors like an offender's criminal history or political rivalries, it primarily focuses on daily crime-related factors.

“Crime Record Management System” by Shah [3]

The objective is to assist law enforcement in digitally storing all case-related information within a centralized database, eliminating the need for manual record-keeping [3]. This system supports three types of users. First, the Administrator, responsible for managing staff/user records and overseeing case listings. Second, the Non-Commissioned Officer (NCO), who handles complaints and assigns cases to specific Criminal Investigation Department (CID) officers. Lastly, the CID officer, tasked with managing and updating investigation details for the cases assigned to them.

“Online Crime Server and Management” by Babar et al. [4]

The Online Crime Management System is designed to digitize the existing manual operations of police stations [4]. The current system has various limitations and inefficiencies due to its reliance on manual record-keeping. This project primarily focuses on automating the process of recording and managing crime-related data, improving efficiency and accuracy in law enforcement operations.

“Criminal Management System” by Jayaswal et al. [5]

The Criminal Management System is built using MySQL, PHP, and the Apache HTTP Server [5]. The primary goal of this project is to significantly improve the efficiency and accuracy of crime recording processes for security agencies. Designed to operate around the clock, this system is accessible to all residents of the country, ensuring continuous availability and reliability.

“Crime Report Management System” by Idhole et al. [6]

This project focuses specifically on crime detection and prevention. The study aims to enhance crime investigations by offering effective and efficient investigative methods [6]. The software development process involves planning, requirement analysis, system analysis, deployment, and maintenance. The Crime Reporting Manager facilitates secure and confidential communication between complainants and authorities, improving the overall reporting and investigation process.

“Crime File System” by Rathi et al. [7]

The project, named "Crime File System," is an application designed to streamline crime reporting. This software enables users to report crimes, file complaints, track the status of their complaints, and stay informed about further legal proceedings [7].

“Online Crime Management & Reporting System” by Ganiron et al. [8]

The Crime Management and Reporting System operates both online and offline while encouraging active citizen participation [8]. This concept is inspired by the challenges of visiting police stations in person and concerns over the authorities' limited investigative efficiency in handling minor crimes, as well as the restricted dissemination of crime-related information within the community.

“AICAMS: Artificial Intelligence Crime Analysis and Management System” by Brahan et al. [9]

This paper explores the creation of a system designed to assist police investigations across various crime sectors [9]. The methodology, originally derived from multiple North American break-and-enter projects, has been tailored to fit the needs of the Hong Kong police. Initially, the system operates on a

rule-based framework, with future enhancements planned through machine learning and neural network techniques to enhance efficiency. Additionally, it leverages existing data sources extensively to support investigations.

"Inside of Cyber Crimes and Information Security: Threats and Solutions" by Maghu et al. [10]

This paper emphasizes the significance of understanding the impact of cybercrime, considering recent incidents, and providing solutions for self-protection [10]. It underscores the importance of cybersecurity and the potential threats posed by such illegal activities. Additionally, the paper presents strategies to address the growing prevalence of cybercrime. The adoption of advanced technologies to safeguard individuals from cyber threats is recommended. Several case studies are analyzed, and innovative cybersecurity measures for the future are proposed.

"Research Aspect of Expert System of Indian Judiciary of Crime Against Women" by Jadhav and Nalwade [11]

This is an intelligent system designed to function by acquiring knowledge and applying it accordingly [11]. It operates within a specific domain to address problems efficiently, utilizing captured information to make informed decisions and provide solutions.

"Cybercrime: Understanding and Addressing the Concerns of Stakeholders" by Martin and Rice [12]

This paper highlights the concerns of computing stakeholders regarding the increasing occurrences of information security breaches and malware attacks, including the rise of sophisticated threats that evade detection [12]. It emphasizes the importance of e-security awareness, education, the role of legal frameworks and law enforcement, and the implementation of up-to-date security software and systems. Additionally, while not always classified as criminal, stakeholders have raised significant concerns about cyberbullying, particularly its impact on younger users and school-aged children.

Limitations of previously proposed systems that our project covers are:

- Updated and detailed records.
- Large data storage.
- Data backup and recovery facility.
- Highly secured with user authentication.
- User interactive and time saving.
- Higher efficiency and accuracy.

METHODOLOGY

The project was initially developed using a waterfall approach, following a sequential, step-by-step process that facilitated smooth progress due to its clear structure. Later, the development of the Crime Management System adopted a well-organized methodology to ensure efficiency, scalability, security, and user-friendliness. By incorporating the Software Development Life Cycle (SDLC), with a focus on Agile principles, the project benefits from iterative development cycles, continuous feedback, and regular improvements. Furthermore, the system is constructed with the MERN stack (MongoDB, Express.js, React.js, Node.js), providing a robust, full-stack JavaScript-based architecture as shown in Figure 3.

Requirement Analysis and Specifications

This is the first step where we analyzed the technologies required and made the specifications for each technology being used. It included installing the required components on our personal computers such as VS code, MongoDB, React, Express.js.

- *MongoDB:* NoSQL Database.
- *Express.js:* Backend Web Framework.
- *React.js:* Frontend JavaScript Library.
- *Node.js:* JavaScript Runtime Environment.

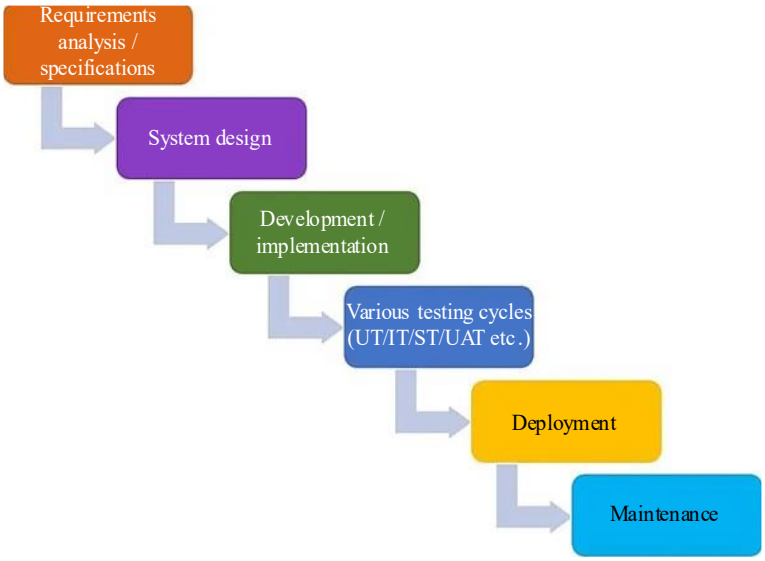

Figure 3. Waterfall methodology.

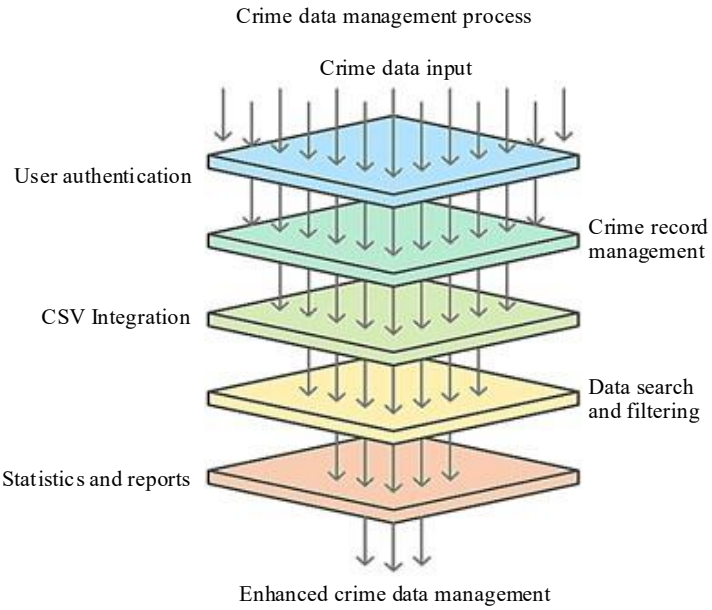

Figure 4. Layered architecture.

System Design

System designing included designing the architecture of our system. Application is made using layered architecture; the designing and functioning of layers are as shown in Figure 4.

The architecture follows a client-server model, where,

- The client (user interface) sends requests for crime data entry, updates, or retrieval.
- The server processes these requests and interacts with the database for persistent data storage.

Here is the architectural design as shown in Figure 5.

Development: The development of application mainly constitutes of the following three phases. It is a three tier architecture:

i. *Frontend Development:* Using React.js to develop an intuitive and responsive user interface with role-based access.

ii. *Backend Development:* Implementing RESTful APIs using Express.js and Node.js to handle business logic and database interactions.
iii. *Database Design:* Using MongoDB to store crime reports, user information, and case statuses efficiently.

Testing and Debugging: Testing is a crucial phase of the development process that ensures the system meets its requirements and functions as expected. The testing strategy for the Crime Management System (CMS) includes various levels of testing to verify the application's functionality, performance, security, and reliability.

Unit Testing

- *Objective:* Verify the functionality of individual components or modules.
- *Example Test Cases:* shown in Table 1.

Integration Testing

- *Objective:* Validate interactions between different modules.
- *Example Test Case:* shown in Table 2.

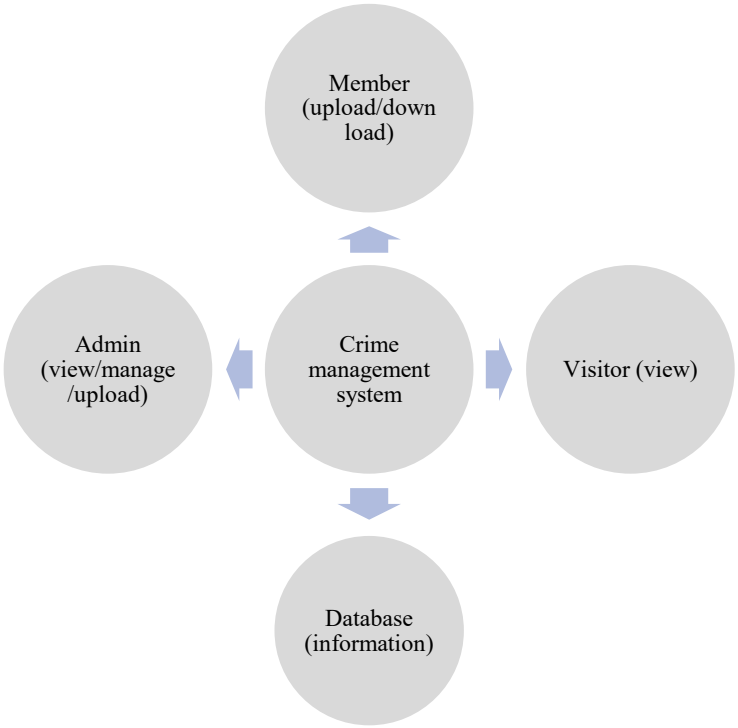

Figure 5. Architectural design.

Table 1. Unit testing test cases.

Test Case ID	Module	Input	Expected Output	Status
UT-001	Login Validation	Correct username/password	Successful login	Pass
UT-002	Login Validation	Incorrect password	Error message: "Invalid credentials"	Pass
UT-003	Add Crime	Valid inputs	Crime added successfully	Pass

Table 2. Integration testing test cases.

Test Case ID	Scenario	Steps	Expected Result	Status
IT-001	Crime record insertion and retrieval	Add a crime record; Retrieve it using search functionality.	Record displayed with accurate details.	Pass

System Testing

- *Objective:* Test the end-to-end functionality of the entire system.
- *Example Scenario:*
  - Log in as Admin.
  - Add a new crime record.
  - Assign a case to an officer.
  - Generate a report for all crimes linked to that case.
  - Verify the report content matches expected data.

Performance Testing

- *Objective:* Measure system responsiveness and stability under varying loads.
- *Example*: As shown in Table 3.

Security Testing

- *Objective:* Ensure the system is secure from unauthorized access and vulnerabilities.
- *Example Security Test Case:* Shown in Table 4.

Deployment and Maintenance: Deploying the system on a cloud server, ensuring scalability, security, and regular updates based on user feedback was the last step of project development. After successfully developing the Crime Management System, it is crucial to focus on long-term maintenance to ensure the system remains functional, secure, and scalable.

Once the application is deployed, ongoing maintenance is required to ensure its performance, security, and scalability. Regular bug fixes and updates should be applied by keeping dependencies up to date and using tools like NPM audit fix to fix vulnerabilities.

RESULTS

The proposed system was tested for efficiency, usability, and security. Performance evaluation showed improved response time in crime reporting and case tracking. User feedback highlighted the ease of use, security, and reliability of the platform. The system successfully reduced paperwork and enhanced law enforcement collaboration.

Table 3. Performance Test Case.

Test Case ID	Scenario	Load Condition	Expected Outcome	Status
PT-001	Search query load	1,000 crime records	Query returns results within 2 seconds	Pass

Table 4. Security Test Case.

Test Case ID	Scenario	Test	Expected Result	Status
ST-001	SQL Injection Prevention	Enter malicious SQL in login field	System rejects input without crashing.	Pass
ST-002	Role-Based Access Control	Login as Officer, try to delete a user	Access denied message displayed.	Pass

Key Achievements

- *User Authentication and Role-Based Access:* Secure login with JWT-based authentication ensures data privacy and role-specific access for citizens, officers, and administrators.
- *Crime Reporting and Tracking:* Users can report crimes with details like location, description, and evidence, while officers can update investigation status.
- *Real-time Case Updates:* Officers and administrators can update crime progress in real-time, providing transparency and accountability.
- *Database Management:* MongoDB efficiently stores and retrieves crime records, allowing for quick data analysis and insights.

- *Scalability and Performance:* The system is deployed on Render/Heroku (backend), Vercel/Netlify (frontend), and MongoDB Atlas (database), ensuring high availability and scalability.
- *Security Measures:* Data protection via bcrypt.js for password hashing, JWT authentication, CORS policies, and Helmet.js enhances security against cyber threats.
- *User-Friendly Interface:* The React-based UI ensures smooth navigation, providing an intuitive experience for users.

This is how the screen is going to look on user's end as shown in Figures 6 and 7.

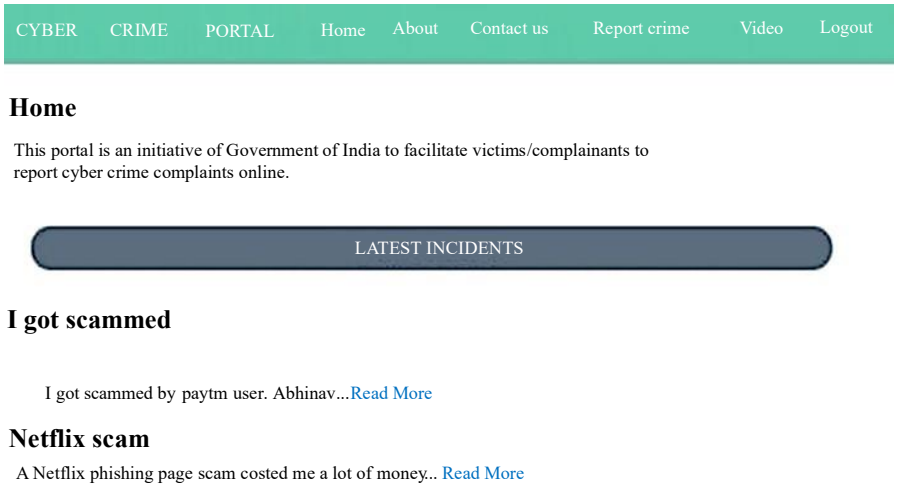

Figure 6. Home page.

Figure 7. Login page.

CONCLUSION

The development of the Crime Management System using the MERN stack demonstrates the power of modern web technologies in solving real-world problems. The system effectively addresses crime reporting challenges by digitizing the process, making it more accessible, transparent, and efficient for citizens and law enforcement agencies. The role-based access system ensures that sensitive information is protected while allowing authorized personnel to perform their respective tasks. The implementation of MongoDB Atlas for cloud-based storage ensures data security and reliability, while the use of React.js for the frontend provides a dynamic and interactive user experience.

Moreover, deployment on cloud platforms enables seamless scalability, ensuring that the system can handle growing numbers of users and crime reports. With proper maintenance strategies such as security updates, performance optimizations, and regular database backups, the system remains stable and secure.

In conclusion, the Crime Management System provides a robust, scalable, and efficient platform that enhances crime reporting and case tracking. Future enhancements could include AI-based crime pattern analysis, real-time notifications for case updates, and integration with law enforcement databases to further improve crime prevention efforts.

Future Scope

The CMS has laid a strong foundation for further development. Several enhancements can be considered for future iterations:

- *Graphical User Interface (GUI):* Developing a user-friendly GUI will improve accessibility and usability for all users, including non-technical personnel.
- *Real-Time Features:* Integrating Geographic Information System (GIS) technology can enable real-time crime mapping and visualization. Adding support for real-time alerts and notifications for ongoing cases or critical incidents.
- *Predictive Analytics:* Incorporating machine learning algorithms can enable the system to analyze historical data and predict potential crime patterns.
- *Mobile Integration:* Developing a mobile application will allow field officers to access and update case information on the go.
- *Inter-System Connectivity:* Integrating with national databases and other law enforcement systems can provide a more holistic view of crime and case data.

REFERENCES

1. Tayal DK, Jain A, Arora S, Agarwal S, Gupta T, Tyagi N. Crime detection and criminal identification in India using data mining Techniques. AI Soc. 2015; 30(1): 117–127.
2. Shiju Sathyadevan, Devan MS, Gangadharan Surya S. Crime Analysis and Prediction using data mining. IEEE *2014* First International Conference on Networks & Soft Computing *(ICNSC2014)*, Guntur, India. 2014 25 Sep; 406–412.
3. Shah BK. Crime record management system. Doctoral dissertation. Sikkim: Shri Ramasamy Memorial University; 2022 Aug.
4. Babar M, Sahare P, Katre R, Ganvir P, Sakharwade B, Chikate R. Research on Online Crime Server and Management. Int J Sci Res Eng Trends. 2021; 7(6): 3476–3483.
5. Jayaswal V, Gupta S, Yadav R, Sharma S. Criminal Management System. Int J Eng Res Comput Sci Eng. 2021; 8(7): 14–19.
6. Idhole MG, Dhawak SW, Rathod RS, Rathod KB, Chavhan KL. Crime Report Management System. Int Res J Mod Eng Technol Sci. 2021; 3(7): 760–764.
7. Rathi A, Gajbhiye S, Dewangan A. Crime File System. Int J Nov Res Dev. 2023; 8(6): f902–f907.
8. Ganiron Jr TU, Chen JS, Dela Cruz R, Pelacio JG. Development of an online crime management & reporting system. World Scientific News (WSN). 2019; 131: 164–80.
9. Brahan JW, Lam KP, Chan H, Leung W. AICAMS: artificial intelligence crime analysis and management system. Knowl-Based Syst. 1998 Nov 23; 11(5–6): 355–61.
10. Maghu S, Sehra S, Bhardawaj A. Inside of Cyber Crimes and Information Security: Threats and Solutions. International Journal of Information and Computation Technology (IJICT). 2014; 4(8): 835–40.
11. Jadhav JS, Nalawade KM. Research Aspect of Expert system of Indian judiciary of crime against women. Int J Eng Sci. 2013; 2(7): 13–17.
12. Martin N, Rice J. Cybercrime: Understanding and addressing the concerns of stakeholders. Comput Secur. 2011 Nov 1; 30(8): 803–14.
13. Chen H, Chung W, Xu JJ, Wang G, Qin Y, Chau M. Crime data mining: a general framework and some examples. Computer. 2004 Apr 30; 37(4): 50–6.
14. Cunningham GM, Harris JE. Toward a theory of performance reporting to achieve public sector accountability: A field study. Public Budg Finance. 2005 Jun; 25(2): 15–42.
15. Ganiron Jr TU, Chen JS, Dela Cruz R, Pelacio JG. Development of an online crime management & reporting system. World Scientific News (WSN). 2019; 131: 164–80.

16. Dintino JJ, Martens FT. Police Intelligence Systems in Crime Control: maintaining a delicate balance in a liberal democracy. CC Thomas; Springfield. 1983.
17. Douglas JE, Burgess AW, Burgess AG, Ressler RK. Crime classification manual: A standard system for investigating and classifying violent crime. John Wiley & Sons; New Jersey. 2013 Mar 26.
18. Eterno JA, Verma A, Silverman EB. Police manipulations of crime reporting: Insiders' revelations. Justice Q. 2016 Jul 28; 33(5): 811–35.
19. Ganiron Jr TU, Manlutac KB, Castro MS, Jerusalem CR. Development of User Guide on Interactive Way-Finder and E-Notices System. World Scientific News (WSN). 2019; 128(2): 363–90.
20. Ganiron Jr TU. Issues and challenges in the College of Architecture, Qassim University towards accelerated learning techniques. World Scientific News (WSN). 2017; 90: 203–30.
21. Gitmed W. Citizens reporting crimes online: The San Francisco experience. Police Chief. 2007 Aug; 74(8): 124, 126–128, 131.
22. Gottschalk P, Tolloczko PC. Maturity model for mapping crime in law enforcement. Electron Gov, An Int J. 2007 Jan 1; 4(1): 59–67.
23. Harvey J, Lau SF. Crime-money, reputation and reporting. Crime Law Soc Change. 2009 Jul; 52(1): 57–72.
24. Haugen S, Roger Selin J. Identifying and controlling computer crime and employee fraud. Ind Manag Data Syst. 1999 Dec 1; 99(8): 340–4.
25. Icove DJ. Automated crime profiling. FBI L Enforcement Bull. 1986; 55: 27–30.
26. Iriberri A, Leroy G, Garrett N. Reporting on-campus crime online: User intention to use. In Proceedings of the IEEE 39th Annual Hawaii International Conference on System Sciences (HICSS'06). 2006 Jan 4; 4: 82a–82a.
27. Iriberri A, Leroy G. Natural language processing and e-government: Extracting reusable crime report information. In 2007 IEEE International Conference on Information Reuse and Integration. 2007 Aug 13; 221–226.
28. Iriberri A, Navarrete CJ. E-government services: design and evaluation of crime reporting alternatives. Electron Gov, an Int J. 2013; 10(2): 171–88.
29. Jamiesona R, Landa LP, Winchestera D, Stephensa G, Steelb A, Maurushatb A, Sarrec R. Addressing identity crime in crime management information systems: Definitions, classification, and empirics. In: Transnational Financial Crime. Routledge; London, England. 2017 Jul 5; 399–414.
30. Jewkes Y, Yar M, editors. Handbook of Internet crime. Routledge; London, England. 2013 Mar 7.

