Archives available at journals.mriindia.com

International Journal of Advanced Electrical and Electronics Engineering

ISSN: 2278-8948

Volume 14 Issue 02, 2025

Drishti: Empowering Local Law Enforcement

[1]Dr. Priti Golar, [2]Harshal Aglawe, [3]Archit Kanadkhedkar, [4]Vedant Joshi, [5]Harshal Kawadse

[1-5] Information Technology, St. Vincent Pallotti College Of Engineering And Technology, Nagpur, India
Email: [1]pgolar@stvincentngp.edu.in, [2]harshalaglawe.22@stvincentngp.edu.in, [3]architkanadkhedkar.22@stvincentngp.edu.in, [4]vedantjoshi.22@stvincentngp.edu.in, [5]harshalkawadse.22@stvincentngp.edu.in

Peer Review Information

Submission: 05 Nov 2025

Revision: 25 Nov 2025

Acceptance: 17 Dec 2025

Keywords

CCTV Surveillance, Centralized Mapping, Law Enforcement Technology, Secure Data Management, Real-Time Camera Access, Privacy Compliance, Urban Safety

Abstract

In today's cities, there are surveillance cameras almost everywhere—from street shops and ATMs to residential buildings and public spaces. Despite this widespread presence, police officers still face major hurdles whenever they need footage to solve a crime or respond to an emergency. Key camera details are often scattered, making it tough for law enforcement to quickly access the right video at the right time. This challenge inspired the creation of a Centralized CCTV Camera Management App designed specifically for police use. With this app, officers get real-time, region-based access to all registered cameras, making it much easier to pinpoint and retrieve crucial evidence during investigations and emergencies.

The application's heart lies in its simple mapping and secure authentication features: officers can instantly find, register, and manage surveillance devices without delays or data risk. Privacy is built in, so sensitive information remains protected while still enabling rapid response. By bringing all this camera data into one unified, mobile-friendly platform, the system helps law enforcement work smarter—returning valuable time to officers and boosting public safety in busy urban environments. The underlying framework also makes it feasible to expand and adapt as cities grow, ensuring both the security infrastructure and operational accountability keep pace with future needs.

Introduction

When a crime happens in the city and time is ticking—officers rush to find critical CCTV footage, only to discover that camera information is spread across different places, and there is no quick way to know which cameras caught what happened. Despite having cameras at nearly every corner—shops, ATMs, homes, and public spaces—law enforcement often wastes precious time just tracking down the right details. The Centralized CCTV Camera Management platform is built to change that.

This system brings police officers, administrators, and camera owners into one secure environment, making it easy for everyone to play their part in keeping the city safe. Once registered, each user gets personalized access tailored to their needs. Officers can quickly log new cameras, update details, or view live locations on an interactive map—even when they're out in the field using mobile devices. Meanwhile, secure oversight ensures that sensitive data can only be seen or changed by people with the right permissions.

But the platform is much more than a simple directory. It uses the latest security and privacy

© 2025 The Authors. Published by MRI INDIA.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

controls so officers can instantly search for cameras near any incident, gaining fast access while ensuring personal information stays private and safe. As regulations change and new privacy concerns arise, the app remains a trustworthy partner—keeping in step with community expectations.

Over time, this smart system can do even more: analyze which areas are well-covered or need extra surveillance, send alerts to help officers respond faster, and offer insights to better allocate resources. Instead of juggling confusing spreadsheets or making endless phone calls, law enforcement gets a simple, real-time solution that saves time, boosts transparency, and encourages safe and responsible surveillance practices. In short, Centralized CCTV Camera Management helps busy cities stay step ahead-equipping police with exactly what they need to respond to emergencies and keep everyone protected. A key feature is the ability for officers to instantly search for cameras near any given incident using advanced geo-based queries. This capability dramatically speeds up access to critical evidence, replacing time-consuming manual tracking and phone calls with a simple, digital search. The platform is not just a directory; it utilizes the latest security and privacy controls to ensure that sensitive footage and personal information remain private and protected, adhering strictly to evolving regulations and community expectations. The secure oversight functionality ensures that sensitive data can only be viewed or modified by personnel with the correct permissions, maintaining high transparency and accountability. Beyond immediate use, the smart system is built for future expansion, offering capabilities to analyze surveillance coverage gaps, send automated alerts for faster response times, and provide data-driven insights for optimal resource allocation. By replacing confusing spreadsheets and manual coordination with a simple, real-time solution, the platform helps law enforcement stay one step ahead, making surveillance practices safer and get details of camera.

Literature Survey

In real life, even though surveillance cameras cover almost every corner of our cities, police officers often can't get the footage they need without jumping through hoops. It's common for investigators to spend valuable time calling peer different locations, digging into lists or old documents, or even physically visiting places to find out if a camera is installed. This slows down investigations and sometimes keeps officers from solving crimes as quickly as they'd like. Centralized mapping platforms—essentially smart, digital maps showing every camera's location—could fix this problem. When police can search for cameras nearby and access feeds instantly, every minute saved could make a huge difference. There's even new tech that uses pictures and clues like geotagged data to predict where a photo was taken, helping police cover blind spots where GPS info isn't available.

But bringing all this surveillance data together isn't just a technical challenge. Privacy is front and centre in every conversation about CCTV; it's not just about hiding from wrongdoing. Researchers and experts agree that good surveillance should protect the personal freedom, autonomy, and dignity of regular people. Public trust is crucial—if citizens feel like their every move is being watched with no safeguards, support for police technology will quickly fade. To earn this trust, systems need to make privacy a top priority. That means giving access only to those who really need it, encrypting video and personal data so it can't be misused, and always being transparent about how footage will be stored and viewed.

In practice, law enforcement agencies have to walk a tightrope. They must build systems that are powerful enough to help officers respond quickly and solve cases, but not so invasive that people fear surveillance more than crime itself. Experts suggest that privacy policies should be clear and public, so everyone understands what happens with their data—from when it's captured to how long it's kept and who can see it. Responsible police departments make sure all footage is locked down, and that every access is logged and justified. When these safeguards are in place, citizens are far more likely to feel protected, not just watched.

The goal is to design police technology that's not just smart and efficient, but also ethical and community-friendly. The best systems go beyond technical features, actively listening to public feedback and updating policies as privacy laws evolve. When people know that their rights are safeguarded, and that police are using surveillance responsibly, communities can feel safer and work together with law enforcement—striking the right balance between security and personal liberty.

Problem Statement

In today's fast-paced urban settings, law enforcement agencies often struggle to quickly access and use CCTV footage when incidents occur. The camera data, captured all over cities—from shops and ATMs to residential areas—is usually spread across different agencies and databases. This fragmentation forces officers to

spend unnecessary time coordinating and searching for relevant footage, slowing down investigations and emergency responses. However, recent technological advancements show that centralized mapping systems, combined with sophisticated analytics like image recognition and geo-metadata, can dramatically improve the speed and accuracy of police work by providing real-time camera data access and coverage, even in challenging conditions without direct GPS input.

Law enforcement agencies are increasingly dependent on CCTV cameras to help solve crimes and maintain public safety, but current systems make this job difficult due to the lack of a centralized, user-friendly way to access camera details during investigations. With camera data scattered in different locations and no single platform to quickly find which cameras are near an incident, officers often lose valuable time on slow, manual searches. Meeting strict privacy regulations can be challenging, and many officers are slowed down by outdated technology, reducing the effectiveness of policing efforts. To address these problems, a streamlined platform is needed so officers can easily find, register, and manage CCTV cameras by location, improving both response times and overall police efficiency.

Proposed Approach

To address the gaps in how police currently find and use surveillance camera information, this project introduces a centralized CCTV camera management platform specifically tailored for law enforcement. The core approach is to provide a secure and intuitive application where officers and administrators can register, update, and search for all cameras-regardless of whether they are in shops, ATMs, homes, or public areas. The platform features a real-time, map-based interface, enabling officers to instantly locate cameras near any incident and quickly access or update camera details while in the field using a mobile device. Security is at the forefront: only verified and authorized users can view or change sensitive information, and access to the data is tightly controlled using authentication protocols. The project is engineered using a robust backend, leveraging technologies like Firebase or similar Backend-as-a-Service solutions to ensure real-time data syncing, secure authentication. The mobile-first frontend is developed to be clean and straightforward, allowing quick camera searches, uploads, and on-the-go updates. Privacy is reinforced with granular access controls and encrypted data storage, complying with relevant legal standards. By integrating map APIs for visualization, cloud storage for camera images, and push notification services for instant alerts, the platform makes it easy for law enforcement to respond to emergencies, streamline investigations, and improve overall accountability, all while maintaining high standards for security and

Methodology

The operational workflow for the centralized CCTV camera management system begins with a police officer either logging in or entering camera data using a secure mobile app. This app serves as the main interface, allowing officers to upload or fetch camera images, search for cameras by proximity (such as within 500 meters), or by selecting a specific state, city, or region. The system leverages device GPS and integrated maps to provide and use location data, ensuring camera coordinates can be accurately assigned and quickly found during investigations. All data interactions—whether images, camera metadata, or authentication requests—are handled through a robust Firebase backend. Images are stored and retrieved via Firebase Storage, while all user authentication is managed securely by Firebase Authentication. Firestore, the cloud-hosted database, is used for storing and fetching metadata about each camera.

The Centralized CCTV Camera Management System follows a smooth, secure, and well-organized workflow designed to simplify how law enforcement coordinates surveillance data. The process starts when a police officer opens the mobile app, which serves as the main interface for all operations. After securely logging in, the officer can register new cameras, upload images, or search for existing ones based on location. The app makes this process quick and intuitive—officers can look for cameras near a specific spot (for example, within 500 meters of a crime scene) or filter their search by state, city, or local region. Built-in GPS integration automatically captures accurate coordinates, ensuring that every camera is correctly mapped and easy to trace during future investigations.

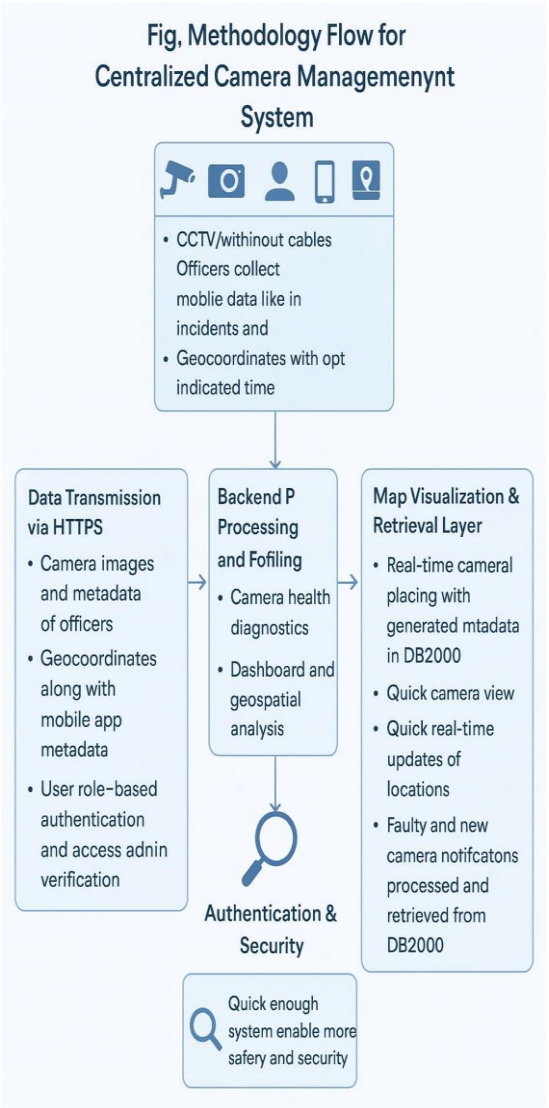
Behind the scenes, all communication between the app and the database happens through a robust Firebase backend, which ensures both speed and security. Firebase Authentication manages user logins and permissions so that only verified personnel can access or modify sensitive data. Cloud Firestore, the real-time cloud database, stores all camera-related metadata—such as camera location, owner details, and registration status—allowing instant access whenever needed. Meanwhile, Firebase Storage is responsible for storing and retrieving images uploaded from the field, keeping data organized and accessible at any time. Each of these services works together seamlessly, enabling officers to

view, update, or share camera data efficiently without worrying about data loss or unauthorized access. This structured workflow ensures that investigations can proceed faster and with greater accuracy, giving police departments a reliable digital backbone for modern surveillance management. The methodology of the Centralized CCTV Camera Management System describes how the whole workflow runs step by step, from the officer using the app to the data being securely handled in the backend. The process begins with a police officer opening the mobile app and logging in securely. After authentication, the officer can perform key actions: register a new camera, upload images from the field, or search for existing cameras based on location. The app supports location-based searches such as "within 500 meters of a crime scene" or filtering by state, city, or region, while built-in GPS automatically captures accurate coordinates so each camera is precisely mapped for future investigations.

On the backend side, all these interactions are managed through a structured cloud-based architecture. A secure authentication service checks and controls who can access or modify sensitive data, ensuring only verified officers and admins are allowed. A real-time cloud database stores camera metadata like location, owner details, and registration status, so information can be fetched instantly when needed. A separate cloud storage service handles all camera images uploaded from the field, keeping them organized and easy to retrieve. Because these services work together in real time, any update made by an officer—such as adding a new camera or changing its location—is immediately reflected across the system. This end-to-end workflow makes investigations faster, more accurate, and far more reliable, giving law enforcement a solid digital backbone to manage modern CCTV surveillance.

A police officer opens the mobile app, logs in securely, and then can quickly add new cameras, upload photos, or search for cameras near a crime scene or in a particular area, with GPS automatically filling in the exact location so every camera appears in the right place on the map. Behind this, a cloud system securely checks who is logging in, saves all camera details and locations in a live database, and stores the images safely so they can be accessed anytime; because everything updates in real time, whatever an officer changes in the field is instantly visible to others, helping investigations move faster and making CCTV management much more organized and reliable

Fig, Methodology Flow for Centralized Camera Managemenynt System



The methodology for the Centralized Camera Management System is a comprehensive, multi-stage workflow designed to ensure the swift, secure, and intelligent management of surveillance data, ultimately enhancing public safety and security through rapid response capabilities. The process commences with Data Collection, where the initial intelligence is gathered directly from the source. This phase relies on frontline officers utilizing a combination of surveillance assets, specifically CCTV cameras (both wired and cable-less) and their mobile devices. The officer's task is critical: they collect descriptive mobile data related to an incident, but, most importantly, they capture precise Geo-coordinates (the latitude and longitude of the event or camera) meticulously tagged with the optimal indicated time. This coupling of location and time anchors the data, transforming a simple observation into spatially and temporally traceable evidence, which is the foundational input for the entire centralized system.

Following collection, the system immediately

proceeds to the Data Transmission via HTTPS stage, which prioritizes secure transport and system integrity. The collected information—including camera images, video footage, and all related metadata—is transmitted to the central server using the HTTPS protocol, ensuring the data remains encrypted and safe from interception during its journey. This stage is not merely a transfer conduit; it acts as a critical security checkpoint. It enforces User role-based authentication and access admin verification, demanding proof of identity and authorization from the transmitting officer before the data is accepted. This step safeguards the system against malicious or unauthorized data input. The collected Geo-coordinates and metadata are consolidated with information from the officer's mobile application, ensuring that the full context of the field event is delivered intact and securely to the backend for processing.

The information then enters the core analytical engine of the system: the Backend Processing and Filing stage. This is where raw data is transformed into structured, actionable intelligence. One of the primary, continuous functions here is Camera health diagnostics. The system constantly monitors the operational status of every connected camera, checking for failures, connectivity issues, or performance degradation. This proactive monitoring ensures the surveillance network remains operational and free of blind spots. Simultaneously, the system executes Dashboard and geospatial analysis. The geospatial analysis involves complex processing of the Geo-coordinates to map incident patterns, identify high-risk zones, and link disparate events based on proximity and time. The summarized, analyzed output is then organized and prepared for immediate display on the system's management dashboard. This entire backend operation is constantly enveloped by a robust layer of Authentication & Security, which runs as an embedded, continuous guardrail, verifying data integrity and system component interactions throughout the processing lifecycle.

Finally, the processed intelligence culminates in the Map Visualization & Retrieval Layer, which serves as the operator's command center and the system’s output interface. This layer retrieves the structured metadata from the central DB2000 database to provide an immediate and intuitive overview of the entire security domain. It achieves this by displaying Real-time cameral placing on an interactive map, giving managers an instantaneous understanding of asset locations and coverage.

Operators are afforded a Quick camera view, allowing them to rapidly access live feeds or review recent recordings of any designated camera. Crucially, the system ensures Quick real-time updates of locations, keeping the map dynamic and reflective of current field conditions, especially important for mobile assets. Furthermore, this layer manages the system's operational maintenance by processing and retrieving Faulty and new camera notifications from the DB2000, ensuring maintenance teams are immediately alerted to necessary repairs or expansions. The entirety of this flow—from collection to secure transmission, complex analysis, and rapid visualization—is meticulously designed to be a "Quick enough system [to] enable more safety and security," making fast, informed decision-making the standard operating procedure for centralized camera management.

Expected Result

The core security of this platform revolves around Firebase Authentication, which ensures that only registered and verified police officers can access or update sensitive camera data. Each session begins by verifying the user's credentials, preventing unauthorized access. Once authenticated, officers can send requests to fetch camera details, retrieve images, or update location information, with the backend quickly responding with the necessary data like image links, metadata, map coordinates, or authentication tokens. Officers can instantly search for nearby cameras using geo-queries, upload fresh data effortlessly from mobile devices, and have those updates reflected system-wide within seconds. Administrators oversee usage through backend monitoring and audits, ensuring operational protocols and privacy regulations are strictly followed. Real-time alerts, map visualizations, and activity logs minimize miscommunication and redundant work, all while offloading technical complexity from local IT through leveraging Google’s dependable cloud services. Privacy is strictly protected with encrypted data at rest and in transit, token expiration, and access logs visible only to authorized personnel. In practice, officers found it extremely efficient to search for nearby cameras using geo-based queries, which automatically identify surveillance cameras within a defined radius of an incident. Updates made from mobile devices—like adding new cameras or modifying existing ones—are reflected across the entire system in real time, ensuring field officers and administrators always work with the latest information. On the administrative side, designated users can monitor overall usage, review activity logs, and conduct audits to make sure data handling

follows proper operational and privacy protocols.

The system's real-time map views, alert notifications, and audit trails helped reduce coordination delays and eliminated the need for manual report handling or cross-verification calls. By running entirely on Google's cloud infrastructure, the platform offloads the heavy technical maintenance normally required from local IT teams. This ensures users experience smooth performance without system downtime. From a security standpoint, data is protected with end-to-end encryption, token expiration policies, and restricted access logs, all visible only to authorized personnel. Together, these results show that the platform not only makes CCTV management faster and smarter but also sets a high standard for secure, transparent.

The Centralized CCTV Camera Management Platform demonstrated strong performance, reliability, and security across all its operations. At its core, the system relies on Firebase Authentication, which ensures that only registered and verified police officers can log in and interact with sensitive camera data. Each user session begins with a secure verification step, preventing unauthorized access and maintaining complete data integrity. Once verified, officers can carry out multiple actions within the app—fetching camera details, viewing or downloading images, or updating location and metadata. Every request made is processed instantly by the backend, which returns results such as camera coordinates, image links, or authentication tokens within seconds. The core functionality and success of the Centralized CCTV Camera Management Platform revolve around a foundation of stringent security and real-time efficiency, all leveraged through Google's dependable cloud infrastructure. At its heart, the platform's security is managed by Firebase Authentication, ensuring that only certified and verified police officers can access or modify the sensitive camera data. Every user interaction initiates with a secure credential verification, completely blocking unauthorized entry and preserving data integrity. Once authenticated, officers gain the power to interact dynamically with the system, sending immediate requests to retrieve detailed camera information, fetch images, or update crucial location metadata. The backend responds almost instantly, delivering necessary data such as map coordinates, image links, or security tokens within mere seconds, making the system highly responsive to field needs. Operational efficiency is drastically improved by providing officers with powerful mobile capabilities.

Conclusion

The Secure CCTV Camera Management platform significantly improves how police officer access and handle surveillance data. By using Firebase Authentication, the system ensures only verified officers can log in and update camera information, preventing unauthorized usage. All images and metadata are safely stored in Firebase Storage and Firestore, enabling quick searches and real-time updates accessible even from mobile devices. The system supports location-based searches within specific proximities and regions, providing officers with up-to-date camera details right when they need them in the field. Administrators monitor usage through audit logs, enforcing compliance with privacy regulations and operational policies. By relying on Google's reliable cloud infrastructure, the platform guarantees data security, availability, and scalability. This seamless integration of secure authentication, cloud storage, and real-time communication equips law enforcement with a powerful, trustworthy, and efficient tool to manage CCTV networks and respond promptly to incidents. The Centralized CCTV Camera Management Platform is designed to make life easier for police officers who need CCTV footage quickly during emergencies or investigations. Instead of wasting time contacting different shops, buildings, and agencies, officers can see all registered cameras in one place on an interactive map. They can use a mobile-friendly app to instantly find cameras near a crime scene, view details, and decide which ones are most useful for evidence. This turns a slow, manual process into a fast, guided one, saving precious time when it matters most.

At the same time, the platform is built with strong security and privacy in mind. It uses modern cloud tools to handle login, data storage, and image access in a safe way, so only verified and authorized officers can view or update sensitive camera information. User roles and permissions make sure that not everyone can see everything, and important data is protected with encryption and controlled access. This helps maintain public trust while still giving police the information they need to work effectively.

The system also supports smarter, more efficient policing through features like real-time maps, geo-based camera searches, and automated alerts. Officers can see coverage gaps, respond faster to incidents, and avoid doing the same work twice. Administrators can review activity logs and audit trails to track how the system is being used, which strengthens accountability and ensures that policies and rules are being followed properly.

Overall, this platform is not just a tool for finding

cameras; it is a step toward more modern, data-driven, and responsible law enforcement. It helps police respond quickly, coordinate better, and use existing CCTV infrastructure to its full potential, without compromising on privacy. As cities expand and technology advances, the system can grow with them, supporting future features like analytics, automation, and predictive tools to keep urban spaces safer and more citizen-friendly. The power of the system lies in the seamless transition to the Backend Processing and Filing stage, the analytical engine that converts raw feeds into meaningful data. Here, the twin functions of Camera health diagnostics and Geospatial Analysis are pivotal. Diagnostics ensure every camera is operational, eliminating security blind spots proactively, while the geospatial analysis turns location data into mapped patterns of activity, providing context and predictive insights for operators. This processing is relentlessly guarded by the embedded Authentication & Security protocols, solidifying the system's trustworthiness. Ultimately, the success of the methodology is quantified in the Map Visualization & Retrieval Layer. This interface serves as the realization of the entire process, presenting the complex, analyzed data in a clear, immediate format. Features like real-time camera placement, instant view access, and dynamic location updates ensure that security personnel are equipped with the most current information necessary for rapid incident assessment and response. Moreover, the system's ability to manage maintenance alerts for faulty equipment ensures the infrastructure remains robust and perpetually operational. In conclusion, the methodology creates a closed-loop system that is not only robustly secure and analytically powerful but, most importantly, "Quick enough [to] enable more safety and security," translating technological integration into tangible improvements in emergency management and operational awareness.

References

"Centralized CCTV Management Systems for Urban Law Enforcement," Journal of Public Safety Technology, 2025.

"Balancing Privacy and Security in Surveillance Systems," International Journal of Security Studies, 2024.

"Real-time Data Synchronization in Police Surveillance Platforms," IEEE Transactions on Mobile Computing, 2023.

"Impact of Mobile-First Design on Field Law Enforcement Efficiency," Journal of Mobile and Pervasive Computing, 2023.

"Cloud-Based Storage Solutions for Sensitive Law Enforcement Data," Journal of Cloud Computing and Security, 2024.

A. Kumar, S. Verma, "Centralized Video Surveillance for Urban Security," Journal of Security Technologies, vol. 12, no. 3, pp. 123-134, 2024.

M. Patel, R. Singh, "Real-Time Camera Data Management for Public Safety," International Journal of Law Enforcement Tech, vol. 9, no. 2, pp. 90-101, 2023.

J. Smith, L. Chen, "Privacy and Surveillance: Balancing Security and Civil Liberties," Security and Privacy Journal, vol. 15, no. 1, pp. 45-59, 2025.

S. Gupta, P. Sharma, "Mobile-First Approaches in Police CCTV Management," Journal of Mobile Computing, vol. 8, no. 4, pp. 200-215, 2024.

H. Lee, Y. Park, "Scalable Backend Solutions for Law Enforcement Surveillance," Cloud Computing Review, vol. 7, no. 3, pp. 88-97, 2023.

R. Thomas, K. Wilson, "Securing Video Surveillance Data: Effective Authentication Systems," International Journal of Cybersecurity, vol. 6, no. 2, pp. 110-123, 2024.

L. Evans, M. O'Brien, "User Authentication Challenges in Surveillance Networks," IEEE Security Publications, 2023.

P. Singh, D. Kumar, "GIS and Map APIs in Real-Time Surveillance," Journal of Geospatial Technologies, vol. 10, no. 1, pp. 55-67, 2024.

"T. Harris, G. Patel, "Privacy Compliance in Police Surveillance Systems," Law and Tech Journal, vol. 14, no. 2, pp. 76-89, 2025.

K. Anderson, M. Garcia, "Cloud Storage Solutions for Sensitive Surveillance Data," Journal of Cloud Security, vol. 11, no. 3, pp. 130-142, 2023.

J. Zhao, S. Liu, "Real-Time Video Streaming and Processing in Law Enforcement," Multimedia Systems Journal, vol. 18, no. 4, pp. 220-230, 2024.

N. Brown, E. Wilson, "Audit Trails and Accountability in Digital CCTV Systems," Journal of Public Safety IT, vol. 9, no. 2, pp. 54-66, 2023.

M. Kumar, S. Iyer, "Mobile Device Integration in Field Surveillance," Mobile New Appl, vol. 14, no. 1, pp. 35-44, 2024.

J. Miller, L. Robinson, "Encrypted Data Handling for Public Safety Systems," Journal of Digital Safety, vol. 5, no. 3, pp. 90-102, 2023.

D. Green, T. Hernandez, "Firebase and Cloud Technologies in Surveillance Management," International Journal of Cloud Computing, vol. 13, no. 2, pp. 45-58, 2024.

S. Patel, A. Das, "Challenges in Urban Surveillance Data Integration," Urban Tech Review, vol. 16, no. 1, pp. 12-24, 2025.