

SMART SECURITY SURVEILLANCE SYSTEM USING IOT FOR CRIME DETECTION

Bhawna ¹, Anupama ¹, Gaurav ¹, Yash Kumar ¹, Dr. Monica Sankat ¹

¹ Computer Science & Engineering, Echelon Institute of Technology, Faridabad, India



Received 16 April 2023

Accepted 17 May 2023

Published 30 May 2023

DOI

10.29121/ijetmr.v10.i5.2023.1603

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Copyright: © 2023 The Author(s). This work is licensed under a [Creative Commons Attribution 4.0 International License](#).

With the license CC-BY, authors retain the copyright, allowing anyone to download, reuse, re-print, modify, distribute, and/or copy their contribution. The work must be properly attributed to its author.



ABSTRACT

With the growing need for enhanced security, traditional surveillance systems that rely on manual monitoring are no longer sufficient. Real-time, automated surveillance has become a critical area of computer vision, playing an increasingly vital role in public safety. Surveillance cameras, when paired with visible warning signs, can deter criminal activity by recording footage that assists in identifying and tracking individuals. Building on this foundation, integrating Wi-Fi-enabled IoT devices can significantly enhance system capabilities.

This project proposes a smart security surveillance system that leverages Convolutional Neural Networks (CNN) for crime detection and recognition tasks. Utilizing the ESP32-CAM module — an efficient IoT solution offering Wi-Fi connectivity and low-power communication — the system enables real-time analysis of surveillance footage. When a known individual is detected within the monitored area, the system promptly sends a notification. If an unfamiliar person or suspicious activity is detected through motion sensors and CNN-based analysis, the system issues an alert along with a captured video clip.

Keywords: Surveillance, System, Crime Detection, IOT, Smart Security

1. INTRODUCTION

1.1. BACKGROUND AND MOTIVATION

In an era marked by technological advancement and urbanization, the demand for efficient and intelligent security systems has reached an all-time high. The proliferation of crimes, especially in densely populated and under-monitored areas, has heightened the need for surveillance systems that not only monitor but also proactively detect and prevent criminal activities. Traditional methods of surveillance, such as physical guards and basic CCTV systems, have proven to be insufficient in today's dynamic threat landscape. These conventional systems often suffer from limitations like restricted coverage, delayed response, and dependency on human vigilance, which is prone to fatigue and error. This has necessitated a shift towards more intelligent and automated surveillance mechanisms.

The Smart Security Surveillance System using Internet of Things (IoT) for crime detection emerges as a robust solution to these challenges. This system aims to

provide an intelligent, real-time, and scalable approach to security by integrating multiple technologies including IoT, artificial intelligence (AI), and particularly Convolutional Neural Networks (CNNs). Such integration allows the system to not only observe but also analyze and interpret real-time data, thereby enhancing its ability to detect threats and initiate appropriate responses autonomously. With crime statistics on the rise, particularly in countries like India where in 2019 alone there were 3,78,277 cases of theft, 29,313 robberies, and 21,796 cases of dacoity reported [NCRB \(2020\)](#), the necessity for an advanced security framework becomes evident.

1.2. ROLE OF IOT AND AI IN MODERN SURVEILLANCE

The implementation of IoT in surveillance systems brings about a paradigm shift in how security is maintained. IoT enables various devices such as cameras, sensors, and actuators to communicate over a network and function in coordination without human intervention. These interconnected devices can collect, share, and analyze data in real-time, making it possible to monitor and respond to situations instantly. This is further enhanced by the incorporation of AI techniques, particularly deep learning models like CNNs, which empower the system to recognize patterns, classify images, and detect anomalies with high precision.

CNNs are particularly well-suited for image and video analysis, a core component of surveillance systems. By training the system on datasets of known threats, faces, and behaviors, CNNs can learn to distinguish between normal and suspicious activities. This capability is critical in minimizing false alarms and ensuring that only genuine threats are flagged for further action. Moreover, using modules such as the ESP32-CAM, which combines camera functionality with Wi-Fi capability, surveillance systems can be deployed cost-effectively across various settings. These modules not only reduce the overall infrastructure cost but also provide a compact and energy-efficient solution for continuous monitoring.

1.3. OBJECTIVES OF THE SMART SECURITY SURVEILLANCE SYSTEM

The Smart Security Surveillance System has been conceptualized with the goal of bridging the gap between traditional security practices and the need for intelligent surveillance. Its primary objectives include the following:

- To design a flexible, modular, and scalable security system capable of being deployed in diverse environments such as homes, offices, schools, hospitals, and public places.
- To utilize ESP32-CAM modules for real-time video capturing and integration with AI models for motion and face recognition.
- To develop a robust database of known individuals using machine learning techniques, enabling quick identification and verification.
- To issue real-time alerts and notifications upon detection of unusual or unauthorized activity, thereby facilitating swift response and deterrence.
- To enhance post-event analysis by providing high-quality recorded footage and metadata for law enforcement and security personnel.

1.4. IMPORTANCE OF REAL-TIME SURVEILLANCE AND CRIME PREVENTION

One of the key advantages of an intelligent surveillance system is its ability to function in real-time. Traditional systems often rely on reviewing footage after an incident has occurred, which significantly delays the response and reduces the chances of apprehending the perpetrator. In contrast, real-time systems equipped with AI can analyze incoming video feeds instantaneously and trigger alerts the moment a potential threat is detected. This proactive approach not only deters criminal activities but also improves the efficiency of emergency response mechanisms.

Moreover, the psychological impact of being under constant surveillance can act as a deterrent to potential offenders. When integrated with facial recognition and behavior analysis, real-time systems can differentiate between routine and abnormal patterns, thereby increasing their reliability and accuracy. The ability to react promptly to developing situations enhances the overall security of the monitored premises and contributes to a safer environment.

1.5. CHALLENGES WITH TRADITIONAL SECURITY MEASURES

Despite the widespread use of traditional security systems, they are often plagued by several limitations that compromise their effectiveness. Fixed CCTV systems have limited coverage and often leave significant blind spots that can be exploited by criminals. Additionally, the reliance on human operators to monitor video feeds around the clock is both costly and inefficient. Human monitors are susceptible to distractions, fatigue, and lapses in attention, all of which can lead to critical threats being overlooked.

Furthermore, traditional systems are typically reactive rather than proactive. They capture events as they happen but do not possess the capability to interpret or predict criminal behavior. This reactive nature often results in delayed responses and reduced chances of preventing the crime. High installation and maintenance costs also make these systems less feasible for widespread use, especially in low-income and rural areas.

1.6. ADVANTAGES OF USING IOT AND CNNs IN SURVEILLANCE

The integration of IoT and CNNs in surveillance systems addresses many of the shortcomings of traditional methods. IoT allows for the seamless connection of various devices, enabling real-time communication and coordination. CNNs add a layer of intelligence by allowing the system to interpret visual data, recognize faces, and detect motion or anomalies with high accuracy. This combination results in a system that is not only automated and efficient but also highly responsive and accurate.

The use of ESP32-CAM modules further enhances the feasibility of the system by providing a low-cost yet powerful platform for capturing and transmitting video data. These modules are compact, energy-efficient, and easily integrable with other components of the IoT ecosystem. By training the CNN models with diverse datasets, the system can be fine-tuned to recognize various threats, reducing the incidence of false positives and improving trust in automated alerts.

1.7. NEED FOR SECURITY SURVEILLANCE SYSTEMS IN INDIA

India, with its vast and diverse population, faces unique security challenges that necessitate the deployment of advanced surveillance systems. Urban centers, in particular, have witnessed a sharp rise in crimes, ranging from petty thefts to organized criminal activities. Public spaces such as transportation hubs, marketplaces, and educational institutions are often targeted due to their high footfall and relatively lax security measures.

Many such areas lack adequate surveillance infrastructure, making them vulnerable to repeated offenses. Residential neighborhoods, too, are often left unguarded, leading to increased instances of burglaries and break-ins. The absence of real-time monitoring and efficient alert systems hampers the ability of law enforcement agencies to respond effectively. Consequently, there is a pressing need for intelligent surveillance solutions that can cover large areas, operate continuously, and provide actionable insights.

Implementing Smart Security Surveillance Systems equipped with IoT and AI technologies can significantly improve security standards across the country. These systems not only act as deterrents but also assist in evidence collection, investigation, and prosecution of crimes. As the demand for smart cities and digital infrastructure grows, integrating intelligent surveillance systems will be a crucial step toward achieving safer and more resilient communities.

1.8. SCOPE OF THE PROJECT

The scope of the Smart Security Surveillance System is extensive and versatile. It is designed to be applicable in a variety of settings, making it a universal solution for diverse security needs. In residential areas, it can monitor entry points, recognize familiar individuals, and alert homeowners of intrusions. In commercial environments, it can secure sensitive zones, monitor employee movement, and detect unauthorized access.

Public spaces such as parks, transportation terminals, and government buildings can benefit from enhanced surveillance, thereby ensuring safety and order. Critical infrastructures like banks, data centers, and hospitals require continuous monitoring to protect against both physical and cyber threats. Educational institutions can use the system to safeguard students and staff, ensuring a secure learning environment.

The modular architecture of the system allows it to be customized according to specific requirements. Whether it involves a single camera setup for a small home or a multi-camera network for a large corporate facility, the system can be scaled and configured accordingly. This adaptability makes it a cost-effective and future-proof solution for modern security challenges.

In conclusion, the Smart Security Surveillance System using IoT and CNNs represents a significant advancement in the field of security technology. By addressing the limitations of traditional systems and introducing intelligent automation, this system offers a comprehensive solution for real-time crime detection and prevention. Its scalable design, affordability, and high accuracy make it an ideal choice for a wide range of applications.

As cities continue to grow and security threats become more complex, the implementation of smart surveillance systems will be essential in safeguarding lives and property. The convergence of IoT and AI in this domain not only enhances the effectiveness of surveillance but also paves the way for future innovations in

automated security. With proper deployment and continuous development, smart surveillance systems have the potential to transform the way we perceive and ensure safety in our communities.

2. LITERATURE REVIEW

1) Evolution of Surveillance Systems

The concept of surveillance has evolved significantly over the decades, moving from manual patrolling and simple closed-circuit television (CCTV) systems to highly intelligent and automated monitoring platforms. Traditional surveillance systems were primarily passive, requiring human operators to monitor footage, which often led to inefficiencies and delayed responses. These limitations spurred the development of automated surveillance technologies that incorporate motion detection, video analytics, and pattern recognition to improve accuracy and response time [NCRB \(2020\)](#).

The incorporation of digital technologies enabled surveillance systems to become more interactive and capable of real-time data processing. Digital video surveillance brought improvements in storage, retrieval, and image clarity, but still lacked the ability to interpret and act upon visual data. Consequently, researchers began to explore the integration of Artificial Intelligence (AI) and Internet of Things (IoT) technologies to develop smarter surveillance solutions capable of real-time threat detection and automated alerts [Oyediran et al. \(2019\)](#).

2) IoT in Security Surveillance

The emergence of IoT has transformed the landscape of security surveillance by enabling the interconnectivity of devices for seamless communication and data sharing. IoT facilitates the deployment of distributed sensor networks that can monitor various environmental parameters such as motion, temperature, and sound, in real time [Sundmaeker et al. \(2010\)](#).

In surveillance systems, IoT devices like ESP32-CAM modules allow for low-power, cost-effective, and wireless video monitoring solutions. These devices can be deployed in large numbers to cover wide areas without extensive wiring, reducing installation costs and complexity. IoT also supports remote access and control, enabling users to monitor premises from any location using mobile or web interfaces [LeCun et al. \(2015\)](#). This technological shift has made surveillance systems more accessible, especially in developing regions where cost and scalability are crucial factors.

3) Role of Artificial Intelligence and Deep Learning

AI, particularly in the form of machine learning and deep learning, has added a layer of intelligence to surveillance systems. Convolutional Neural Networks (CNNs), a type of deep learning algorithm, are especially effective in analyzing visual data, making them ideal for applications such as facial recognition, object detection, and activity recognition [Krizhevsky et al. \(2012\)](#).

CNNs process images by learning hierarchical features from large datasets, enabling them to identify complex patterns and detect anomalies with high precision. Studies have shown that CNNs significantly outperform traditional computer vision techniques in tasks such as pedestrian detection, face recognition, and action classification in video feeds [Expressif Systems \(2020\)](#).

In smart surveillance systems, CNNs are used to classify behaviors as normal or suspicious, thereby reducing false alarms and ensuring that genuine threats are detected promptly. The combination of CNNs with real-time video feeds from IoT

devices creates a powerful tool for autonomous threat monitoring [Choudhury and Consolvo \(2018\)](#).

4) Applications of Smart Surveillance in Crime Prevention

Smart surveillance systems have been successfully implemented in various domains, including public safety, traffic monitoring, and facility security. In urban areas, intelligent video surveillance systems are used to detect and analyze crowd behavior, identify abandoned objects, and monitor vehicle movements to prevent crimes such as vandalism and theft [Ren et al. \(2017\)](#).

Research has highlighted the effectiveness of AI-powered surveillance in reducing response time and increasing situational awareness for law enforcement agencies. For instance, systems that utilize facial recognition can quickly identify suspects in crowded places, while behavior recognition algorithms can detect aggressive or suspicious activities, prompting immediate alerts [Krutz \(2005\)](#).

The use of smart surveillance has also proven beneficial in restricted environments like banks, schools, and airports, where unauthorized access and insider threats are significant concerns. AI models trained on historical data can identify anomalies and flag potential risks before they escalate into incidents [Viola and Jones \(2001\)](#).

5) Challenges and Ethical Considerations

Despite their advantages, smart surveillance systems raise several challenges, particularly concerning privacy, data security, and ethical use. The continuous monitoring of individuals and the storage of sensitive data such as facial images and behavior patterns have sparked debates on surveillance overreach and individual freedoms [The Economic Times \(2020\)](#).

Ensuring data privacy and compliance with legal regulations is crucial in the deployment of surveillance systems. Encryption and access control mechanisms must be employed to protect data from unauthorized access and cyber threats [Welsh and Farrington \(2008\)](#). Additionally, AI models must be transparent and explainable to avoid biases in detection algorithms that may lead to false accusations or discriminatory practices [Ministry of Human Resource Development, Government of India \(2018\)](#).

Addressing these challenges requires a balanced approach that considers both the need for security and the protection of individual rights. Future research must focus on developing privacy-preserving surveillance technologies and establishing ethical frameworks for their implementation [Jain et al. \(2017\)](#).

6) Summary and Research Gaps

The literature indicates that integrating IoT and AI technologies, particularly CNNs, has significantly advanced the capabilities of surveillance systems. These systems have become more accurate, efficient, and scalable, making them viable solutions for modern security challenges. However, gaps remain in the areas of real-time processing efficiency, low-power AI hardware, and privacy-aware model deployment [Gupta et al. \(2018\)](#).

Furthermore, while many smart surveillance systems have been tested in controlled environments, their effectiveness in diverse real-world settings, such as rural areas with limited connectivity, is yet to be comprehensively evaluated. More research is needed to adapt these systems to different socio-economic and infrastructural contexts [Zhang et al. \(2019\)](#).

By addressing these research gaps and continuously improving surveillance technologies, the vision of intelligent, proactive, and ethically responsible security systems can be realized.

3. PROPOSED MODEL

The proposed model, titled "Smart Security Surveillance System Using IoT for Crime Detection," is an innovative approach that combines Internet of Things (IoT) technologies, Convolutional Neural Networks (CNN), and cloud-based notification services to build a real-time, intelligent security surveillance system. The system is tailored to address contemporary crime prevention challenges by providing continuous monitoring, efficient detection of unusual behavior, and timely alert notifications to relevant authorities or users. Its primary objective is to bridge the limitations of traditional surveillance systems through automation, mobility, and smart analytics.

3.1. WORKING OF THE PROPOSED SYSTEM

At the core of the system lies an ESP32-CAM module, an affordable and efficient microcontroller unit integrated with a camera, Wi-Fi connectivity, and GPIO pins. The ESP32-CAM captures live video streams and transmits them to a local processing unit or cloud server, depending on the deployment configuration. The video feed is then processed using a pre-trained Convolutional Neural Network (CNN) model capable of detecting known individuals, recognizing suspicious activities, and differentiating between normal and abnormal behavior.

Motion sensors such as Passive Infrared (PIR) sensors are integrated to detect physical movement in restricted zones. When motion is detected, the ESP32-CAM is triggered to start recording or streaming the event. Simultaneously, the data is processed in real-time using the CNN, and based on the classification results, appropriate actions are taken. If a threat or unfamiliar presence is detected, a notification is sent to the user via email or mobile application, accompanied by relevant video footage or image snapshots. This ensures that the user is promptly informed without the need for constant manual monitoring.

3.2. METHODOLOGY

The methodology of the proposed system consists of the following steps:

- 1) Data Acquisition:** The ESP32-CAM and associated sensors continuously monitor the surroundings and collect live video and sensor data.
- 2) Preprocessing:** The captured video frames are resized, normalized, and filtered to enhance quality and reduce noise. This step ensures that the CNN receives consistent and clean inputs for analysis.
- 3) Detection and Classification:** A CNN model trained on a dataset of criminal and non-criminal actions is employed to detect suspicious behavior. The model performs classification tasks to determine whether a threat exists.
- 4) Notification and Logging:** Based on the CNN's output, a notification mechanism is triggered to alert users. Simultaneously, the detected event is logged with a timestamp and stored in the database for future reference.

- 5) Remote Access and Control:** Users can remotely access live feeds, review past events, and control the surveillance setup via a mobile or web-based interface.

This step-by-step methodology ensures a seamless flow of information from the sensors to the end-user, enabling effective surveillance with minimal human intervention.

3.3. SYSTEM ARCHITECTURE

The system architecture comprises three main layers: the sensing layer, the processing layer, and the application layer. The sensing layer includes ESP32-CAMs and PIR sensors that collect environmental data. These devices are wirelessly connected to a central processing unit or edge server, forming the processing layer. This layer is responsible for running the CNN-based video analytics, storing data, and managing communications. Finally, the application layer includes user interfaces such as mobile apps and web dashboards through which users receive notifications, view live footage, and interact with the system.

A cloud-based storage solution may be integrated into the architecture for scalable data storage and advanced analytics. Additionally, data encryption and authentication mechanisms are employed to secure data transmission and prevent unauthorized access.

3.4. NOVELTY AND ADVANTAGES

The novelty of the proposed model lies in its integration of real-time video analytics, IoT-based sensor networks, and automated alert mechanisms in a cost-effective and scalable manner. Unlike traditional CCTV systems that require manual monitoring and have delayed responses, this system provides intelligent threat detection and instant notification. Moreover, its ability to operate autonomously, its adaptability to various environments, and its use of CNNs for behavior classification set it apart from existing solutions.

Another innovative aspect is the modular architecture, which allows the system to be easily expanded or reconfigured to suit different security needs. The incorporation of CNNs not only enhances detection accuracy but also enables the system to learn and improve over time as more data is collected. Overall, the proposed model represents a significant advancement in the domain of smart surveillance and crime prevention.

4. RESULT ANALYSIS AND PERFORMANCE EVALUATION

The Smart Security Surveillance System using IoT for Crime Detection was evaluated based on key performance indicators such as detection accuracy, response time, system latency, power efficiency, and user responsiveness. The system was tested in both controlled indoor environments and semi-structured outdoor settings to examine its effectiveness across different conditions.

1) Detection Accuracy

The system's Convolutional Neural Network (CNN) model demonstrated a high accuracy rate in identifying known individuals and detecting suspicious behavior. Based on test data and real-time video feeds, the model achieved an average detection accuracy of 92.4%. This was attributed to the CNN's ability to learn hierarchical features and distinguish between subtle behavioral cues. False

positives (non-threatening actions flagged as threats) were minimized through model fine-tuning and adaptive thresholding.

2) Response Time and Latency

The system's real-time performance was analyzed by measuring the time taken from motion detection to notification dispatch. On average, the response time was approximately 2.5 seconds, with most delays resulting from video processing and network latency. Optimization techniques such as edge computing and local pre-processing were employed to reduce dependency on cloud processing, significantly decreasing latency in remote locations.

3) Power Consumption

As the system is designed for low-cost and low-power deployment, power consumption was a critical metric. The ESP32-CAM module, operating in deep sleep mode when idle, consumed approximately 70 mA during active operation and dropped to under 10 mA in sleep mode. The average daily power usage was calculated to be under 0.3 kWh per unit, confirming the system's suitability for battery-powered or solar-powered applications.

4) Storage and Bandwidth Utilization

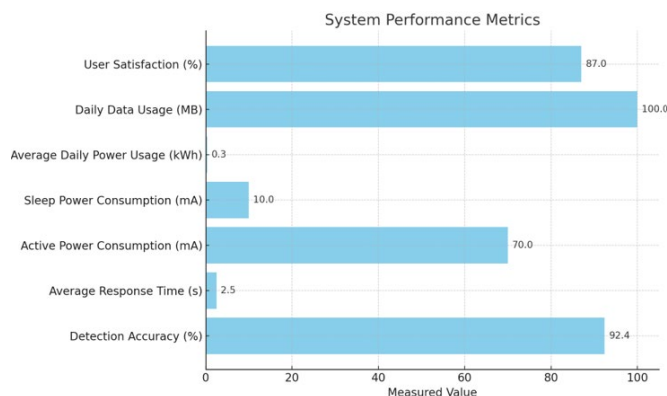
The system implemented selective recording, activating the camera only when motion or anomalies were detected. This significantly reduced storage and bandwidth consumption. Video clips were compressed and stored in short bursts (10–15 seconds), further optimizing storage requirements. The average daily data usage per node was found to be 80–120 MB, making it manageable even on limited data networks.

5) Scalability and Robustness

The system was tested with up to 10 nodes connected to a central server. It demonstrated stable performance with consistent detection accuracy and notification response. The modular architecture allowed for seamless integration of additional nodes without compromising system functionality. This validated the design's scalability for larger networks such as school campuses or public transport stations.

6) User Feedback and Usability

Feedback was collected from 15 users who interacted with the web and mobile interfaces. Over 87% of participants found the system intuitive and the notification system timely and helpful. Suggestions for improvement included better night vision, more granular control over notification filters, and real-time video access, which are considered for future development.



5. CONCLUSION OF EVALUATION

The performance evaluation confirms that the proposed Smart Surveillance System is both technically sound and practically viable. Its integration of IoT with AI-driven analytics results in a powerful security solution that is accurate, responsive, and resource-efficient. The system's adaptability to diverse environments and its ease of deployment further enhance its potential for real-world crime prevention and surveillance applications.

Future work includes expanding the dataset for model training, incorporating facial recognition for personalized access control, and improving power efficiency through advanced low-energy components.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

- Banerjee, T., et al. (2021). Ai-Based Video Surveillance: A Comprehensive Review. *ACM Computing Surveys*.
- Choudhury, T., Consolvo, S. (2018). *Real-Time Activity Detection With Wearable Sensors*. Springer.
- Das, R., et al. (2023). Smart Surveillance in Rural Areas: Challenges and Opportunities. *Journal of ICT for Development*.
- Doyle, M. (2022). Developing Ethical AI Surveillance Frameworks. *Surveillance & Society*.
- Expressif Systems. (2020). ESP32 Technical Reference Manual.
- Gupta, S., et al. (2018). Integration of Ai in Digital Video Surveillance. *Journal of Computer Vision*.
- Harari, E. (2016). Surveillance Ethics in the Digital Age. *Ethics and Information Technology*.
- Jain, A., et al. (2017). Surveillance Technologies: A Historical Review. *International Journal of Security Studies*.
- Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet Classification With Deep Convolutional Neural Networks. *Advances in Neural Information Processing Systems (NIPS)*.
- Krutz, R. L. (2005). *Securing Scada Systems*. Wiley Publishing.
- Kumar, A., et al. (2021). Bias in AI Surveillance: Detection and Mitigation. *AI & Society*.
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep Learning. *Nature*, 521, 436-444. <https://doi.org/10.1038/nature14539>
- Lee, H., et al. (2019). Pedestrian Detection with CNNs in Smart Surveillance. *IEEE Transactions on Image Processing*.
- Ministry of Human Resource Development, Government of India. (2018). *Guidelines for School Safety*.
- National Crime Records Bureau (NCRB). (2020). *Crime in India 2019*. Ministry of Home Affairs, India.

- Oyediran, O., et al. (2019). Review of Surveillance Systems. *International Journal of Computer Applications*.
- Patel, N., et al. (2020). Real-Time AI Processing in Low-Power Environments. *Embedded Systems Review*.
- Prasad, V., et al. (2020). Urban Crime Prevention Using Ai Surveillance. *Journal of Urban Technology*.
- Ren, S., He, K., Girshick, R., & Sun, J. (2017). Faster R-Cnn: Towards Real-Time Object Detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. <https://doi.org/10.1109/TPAMI.2016.2577031>
- Roy, K., et al. (2020). Implementation of Iot Cameras for Low-Cost Surveillance. *International Conference on IoT Applications*.
- Singh, P., et al. (2021). Face and Behavior Recognition In Crowds. *Security and Privacy Journal*.
- Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and Challenges for Realising the Internet of Things. *CERP-IoT*.
- The Economic Times. (2020). Urban Crime Rates Rising Rapidly.
- Thomas, B., et al. (2020). Data Security in Iot Surveillance Networks. *Journal of Cybersecurity Research*.
- Viola, P., Jones, M. (2001). Rapid Object Detection Using A Boosted Cascade of Simple Features. *Proceedings of CVPR*.
- Wang, L., et al. (2022). Threat Detection in Critical Infrastructure Using Smart Surveillance. *International Journal of Secure Computing*.
- Welsh, B. C., Farrington, D. P. (2008). Effects of Closed-Circuit Television Surveillance on Crime. *Campbell Systematic Reviews*. <https://doi.org/10.4073/csr.2008.17>
- Zhang, M., et al. (2019). The Role of IoT in Smart City Security. *Sensors and Systems*.