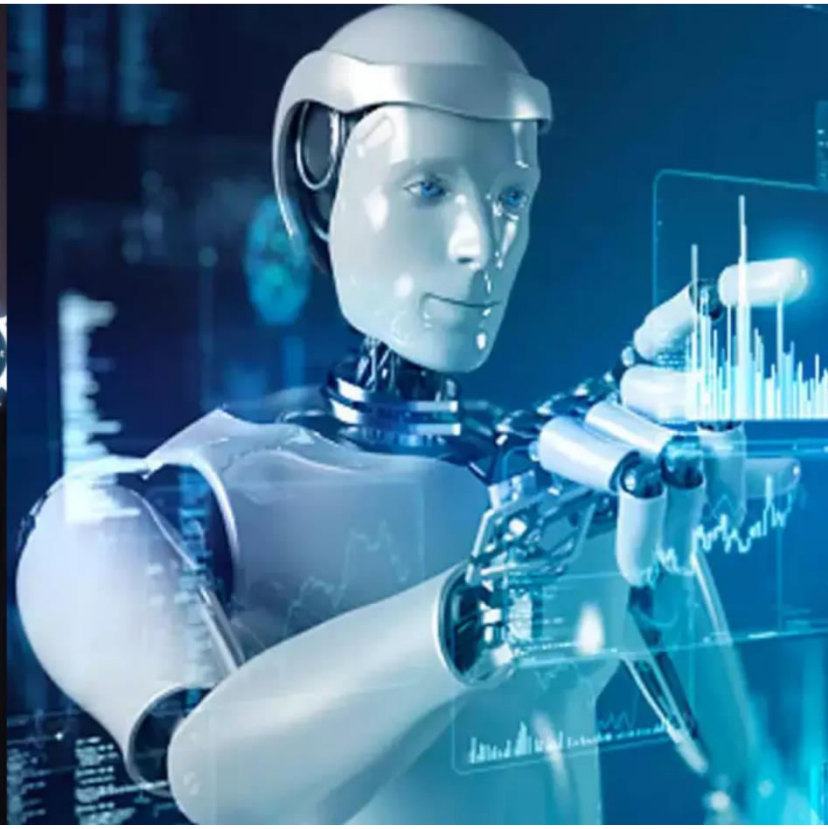
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*

**Impact Factor: 8.699**

**Volume 14, Issue 5, May 2025**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405073|

# Automated Surveillance System using AI

**Dr. Krishnareddy K R**

Head of the Department, Department of Computer Science, S.J.M.I.T, Chitradurga, Karnataka, India

**Darshan H M, Kavya M S, Sindhoora Kalmata, Suprith S**

BE, 8th Semester, Department of Computer Science Department, SJMIT, Chitradurga, Karnataka, India

**ABSTRACT:** This Project explores the integration of artificial intelligence (AI) into decision support systems for personal finance management. As financial landscapes become increasingly complex, traditional approaches often fail to keep pace with evolving market conditions and diverse individual goals. AI- driven systems offer a promising solution by leveraging advanced algorithms to analyze data and provide personalized recommendations. These systems aim to enhance budgeting, investment strategies, debt management, and retirement planning, thereby empowering individuals to make more informed financial decisions and improve their overall financial health. However, challenges such as data privacy and transparency must be addressed to ensure the responsible deployment of these technologies. This research underscores AI's transformative potential in financial technology, highlighting its role in revolutionizing personal finance risk management practices.

The advancement of AI-powered surveillance systems signifies a pivotal shift in the field of security technology. These systems leverage real-time monitoring, anomaly detection, and predictive analytics to proactively identify and mitigate threats, offering a level of responsiveness and accuracy beyond traditional surveillance methods. However, the implementation of such intelligent systems necessitates a balanced approach, with careful attention to ethical considerations, particularly regarding data privacy, algorithmic transparency, and the potential for misuse. Ensuring compliance with legal standards and maintaining public trust through transparency and accountability is essential. As AI continues to evolve, ongoing research and development are critical—not only to enhance system performance and adaptability but also to establish responsible frameworks that protect individual rights while strengthening public safety.

**KEYWORDS:** Surveillance, Security, Warning, Reminder.

## I. INTRODUCTION

The integration of artificial intelligence into surveillance systems marks a significant leap in monitoring capabilities. By leveraging advanced technologies such as machine learning, computer vision, and natural language processing, AI-driven surveillance systems can perform complex tasks like object detection, facial recognition, behavior analysis, and real-time anomaly detection with high accuracy and speed.

These systems are increasingly used in diverse domains, including public safety, traffic management, retail security, and organizational monitoring. Unlike traditional methods, AI-powered surveillance can analyze vast volumes of data, recognize patterns, and predict potential threats, enabling proactive responses and improved operational efficiency.
One of the key advantages of AI surveillance is its scalability and adaptability, making it suitable for various environments—from urban public spaces to private enterprises. Moreover, it contributes to broader societal benefits such as optimizing emergency responses and improving traffic flow in congested areas.

However, the rise of AI in surveillance also brings significant ethical, privacy, and data security concerns. Without proper oversight, these systems risk enabling mass surveillance, reinforcing societal biases, and infringing on individual freedoms. The potential misuse of AI tools underscores the need for strict regulatory frameworks, transparency, and ethical guidelines.

As the technology continues to evolve, balancing innovation with accountability is essential. Ensuring that AI surveillance systems respect individual rights and comply with data protection laws will be crucial in maintaining

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405073|

public trust. Ultimately, while AI-powered surveillance holds the promise of enhanced security and efficiency, its deployment must be guided by a commitment to ethical responsibility and civil liberty.

## II. LITERATURE SURVEY

The system reviews multiple research papers on AI surveillance, each contributing insights into biometric authentication, anomaly detection, and hybrid AI-human monitoring models. Some of the key takeaways includes.

[1]. This paper examines the advancement and application of AI-driven surveillance systems (AISS) aimed at improving security and monitoring across diverse settings. Utilizing 360-degree camera systems and cutting-edge object recognition techniques, the study outlines approaches for identifying suspicious behaviour through biometric verification methods, such as facial and voice recognition. The research also explores key challenges including privacy implications, system scalability, and the risk of false alerts in AI operations. To address these issues, enhancements to existing surveillance technologies are suggested. The paper proposes a hybrid model that combines automated surveillance with human intervention, presenting it as an effective strategy for balancing security needs with privacy protection.

[2]. The rise of smart cities and heightened security requirements following the COVID-19 pandemic have driven the implementation of advanced AI-based surveillance technologies. Numerous studies have investigated the capabilities of these systems in reducing risks and promoting public safety. For example, surveillance systems powered by deep learning, incorporating facial recognition and object detection, have demonstrated high accuracy levels—up to 97% for detecting faces and 99.3% for identifying them. These AI systems provide greater adaptability and are more economical compared to conventional surveillance approaches. Nonetheless, limitations such as the lack of human intuition and the complexity of managing such systems continue to pose significant challenges.

[3]. This research introduces a Temporal Convolutional Network (TCN)-driven approach for real-time surveillance tailored to public safety use cases. By employing biometric methods such as facial recognition and motion tracking, the system detects potentially suspicious behavior and enables intelligent monitoring using tools like Convolutional Neural Networks (CNNs) and OpenCV. The solution minimizes the need for manual oversight while improving performance in terms of accuracy, scalability, and operational efficiency.

[4] "SecureVision" combines AI-powered computer vision with machine learning techniques to provide reliable and equitable surveillance across both public and private environments. It incorporates capabilities such as facial identification, behavior monitoring, and audio analysis to detect and report abnormal activities. With a focus on data protection through encryption and adherence to privacy laws, the system is designed to promote safety while tackling issues related to scalability and ease of use. This paper also explores the growing impact of machine learning in advancing surveillance technologies and its wider significance for urban security and governance.

[5] This study centers on creating affordable AI-enabled surveillance solutions by employing deep learning architectures such as SSD and MobileNets for object recognition and tracking. Core functionalities include gaze tracking and movement analysis, which play a vital role in detecting irregular behaviour. The paper highlights the importance of maintaining a balance between enhanced security, user confidence, and system accessibility, while also tackling challenges like data privacy and false alarm rates. Future work aims to boost the systems' processing efficiency and resilience to better serve a variety of security scenarios.

## III. METHODOLOGIES

The methodology involves collecting and preprocessing video data from surveillance cameras, followed by training models such as SSD or MobileNets for real-time object detection and tracking. Facial recognition and gaze estimation modules are integrated to identify individuals and analyse behaviour. The system uses motion analysis algorithms to detect anomalies, and results are validated against benchmark datasets to assess accuracy and reduce false positives.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405073|

**1. Model Loading**

- Initialize TensorFlow.js (tf.ready()).
- Load the COCO-SSD object detection model.
- Handle success or failure (update isLoading or error).

**2. Webcam Initialization**

- Request webcam access using navigator.mediaDevices.getUserMedia().
- Bind the webcam feed to a <video> element.
- Set the dimensions of the <canvas> elements for drawing overlays and snapshots.

**3. Object Detection**

- Use the loaded model to analyse the video feed frame-by-frame.
- Filter objects based on:
- Class (e.g., person, vehicle).
- Confidence score threshold (CONFIDENCE_THRESHOLD).
- Draw bounding boxes and labels around detected objects.

**4. Incident Detection**

- Analyze the detected objects for specific scenarios:
- Overcrowding: Detect if the number of people exceeds a threshold (CROWD_THRESHOLD).
- Accidents: Detect overlapping bounding boxes of vehicles.
- Fire: Analyze pixel colors or detect fire-related objects.
- Object Movement: Detect specified objects like phones or bags.
- Calculate confidence and log incidents.

**5. Fire Detection**

- Analyse the video frame for red/orange pixel clusters.
- Compute the percentage of fire-like pixels (FIRE_PIXEL_THRESHOLD).

**6. Collision Detection**

- Check if bounding boxes of vehicles overlap.
- Return pairs of overlapping vehicles.

**7. Alert Handling**

- Capture the video frame as evidence.
- Log the incident with details (type, confidence, timestamp).
- Send alerts and images to the configured Telegram chats.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405073|

**4. Data Flow Diagram**

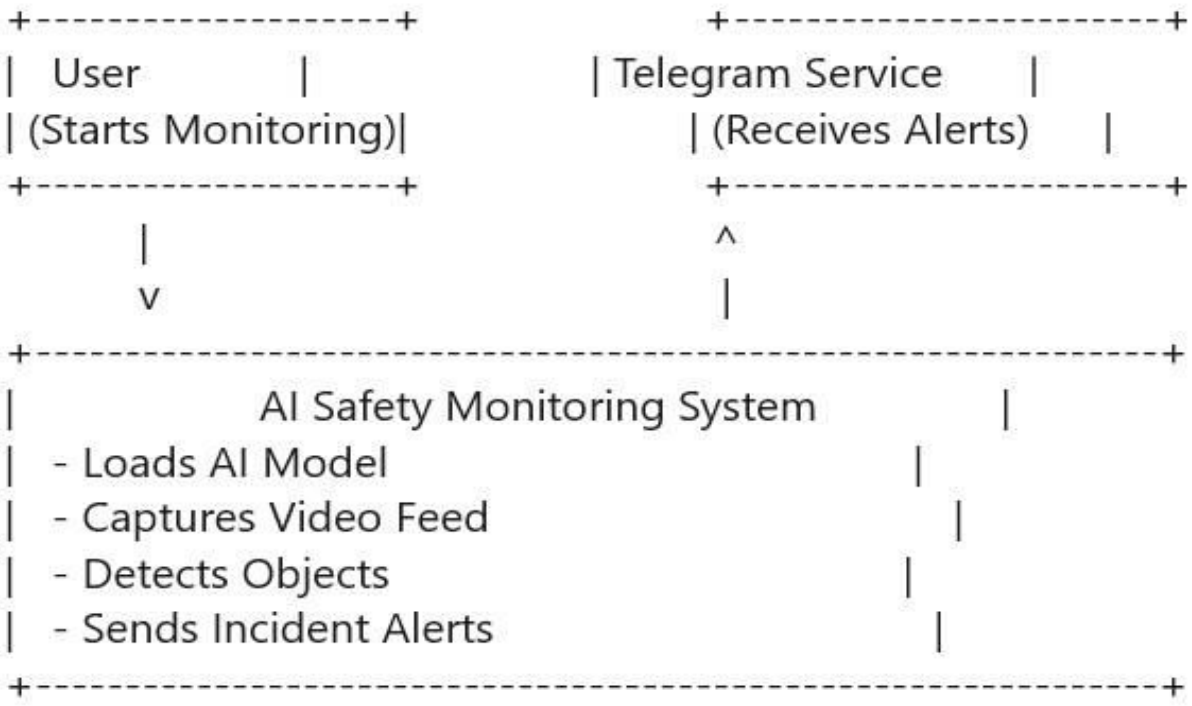



**Figure: Data Flow Diagram**

1. **User:** Initiates monitoring by starting the AI-based safety system.
2. **AI Safety Monitoring System:** Loads the trained AI model for object detection. Captures real-time video feeds for analysis. Detects potential incidents (e.g., overcrowding, fire, collisions) using the model. Sends incident alerts when thresholds are exceeded.
3. **Telegram Service:** Receives alerts (text and images) from the AI system and notifies the user in real-time. the rise of AI-powered surveillance also raises significant concerns about privacy, data security, and ethical use. Misuse of these systems could lead to mass surveillance, bias, and violations of individual freedoms. As the adoption of AI-driven monitoring grows, it is crucial to establish robust regulations and ethical frameworks to balance innovation with accountability and protect privacy rights. . the rise of AI-powered surveillance also raises significant concerns about privacy, data security, and ethical use. Misuse of these systems could lead to mass surveillance, bias, and violations of individual freedoms. . As the adoption of AI-driven monitoring grows, it is crucial to establish robust regulations and ethical frameworks to balance innovation with accountability and protect privacy rights.

## IV. USER MODEL

**1. Preprocessed Datasets**

Represents the training data used to develop the Machine Learning (ML) model. The ML model is trained on these datasets to detect objects and incidents (e.g., fire, overcrowding, collisions**).**

**2. Trained ML Model**

The Machine Learning model (e.g., COCO-SSD or a custom model) is deployed to process live video streams. It is hosted within the system (possibly on the cloud or Raspberry Pi).

**3. Web Application**

Provides an interface for users to interact with the system. Acts as a middleware to manage the communication between users, the trained ML model, and the alerting mechanism. Facilitates access to live video feeds, detection results, and incident history.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405073|

**4. Raspberry Pi**
Functions as the hardware platform for the system. Hosts the web application and ML model to process incoming surveillance videos. Performs the computations locally to analyze video feeds in real time.

**5. Process Surveillance Videos**
The live video feed from cameras is sent to the Raspberry Pi for analysis. The ML model detects objects, evaluates incidents, and processes conditions such as:

- Overcrowding, Vehicle collisions, Fire detection, Object movement

**6. Condition Check**
A decision-making module analyzes the detection results. If incidents meet specific thresholds (e.g., confidence levels, crowd density, collision probability), the system triggers alerts. Two conditions are possible: Normal: No critical incidents detected; no action taken. Alert: A critical incident is detected, triggering the alerting system.

**7. Alerting System**
Sends real-time alerts to users when an incident is detected. Two-Level Alerting Checks: First, verifies the confidence of the detection. Second, confirms incident severity to avoid false alarms.

**8. Internet and Users**
Internet: Connects the system to external devices, allowing remote users to receive alerts and monitor video feeds. Users (User 1, User 2, User 3): Represents the end-users of the system (e.g., safety officers, administrators). They access the system via the web application and receive notifications through the alerting system.

**6. Proposed System**
To address the challenges posed by AI-powered surveillance, it is essential to develop a framework that ensures responsible, ethical, and transparent use of these technologies. This includes implementing robust privacy protections, reducing algorithmic bias through diverse and representative training datasets, and enforcing strict regulations to prevent misuse. The proposed solution focuses on leveraging AI's potential for enhancing security while safeguarding civil liberties, promoting accountability, and fostering public trust in surveillance systems

- **Enhanced Security & Threat Detection:** Detect unauthorized access, suspicious behavior, and potential threats in real time. Identify weapons, intrusions, or hazardous objects using AI-powered vision models.
- **Real-Time Monitoring & Response:** Provide 24/7 surveillance with automated alerts to security personnel. Enable quick response through automated actions like triggering alarms or locking doors.
- **Anomaly & Behavior Detection:** Recognize unusual movement patterns, loitering, or aggressive behavior. Detect unattended objects or abandoned bags in high-risk areas.
- **Facial & Object Recognition:** Identify known suspects, VIPs, or employees for access control. Detect vehicles, license plates, and objects of interest.
- **Privacy-Preserving Surveillance:** Ensure compliance with data privacy laws (GDPR, CCPA) using AI-driven anonymization. Implement role-based access for viewing sensitive data.
- **Crowd & Traffic Analysis:** Monitor crowd density to prevent stampedes or overcrowding. Analyze traffic flow for better urban planning and congestion control.
- **Edge AI for Low Latency Processing:** Utilize edge computing for real-time threat detection without relying on cloud processing. Reduce bandwidth usage by processing data locally before sending alerts.
- **Integration with Law Enforcement & Emergency Services:** Provide seamless integration with police, fire departments, and medical responders. Share real-time footage and incident reports for faster decision-making.
- **Cybersecurity & Anti-Tampering Measures:** Protect surveillance systems from hacking, tampering, or unauthorized access. Use AI-driven cybersecurity solutions to detect and mitigate threats.
- **Scalability & Automation:** Deploy AI-powered surveillance across multiple locations with cloud-based scalability. Automate surveillance tasks to reduce dependency on human monitoring.

**7. System Architecture:**
The proposed system consists of several interconnected components:

- **Surveillance Cameras**: High-definition cameras with 360-degree views collect video data.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405073|

- **AI Processing Unit**: A powerful server or cloud infrastructure runs deep learning algorithms for object detection, facial recognition, and anomaly detection.
- **Data Storage**: Encrypted databases store processed data and video footage, ensuring both security and privacy.
- **User Interface**: An intuitive dashboard allows authorized users to view real-time footage, receive alerts, and review past events.
- **Alerts & Notifications**: The system sends notifications to security personnel or relevant authorities in case of identified threats or unusual activities.

**8. Benefits of the Proposed System:**

- **Efficiency**: Automated detection reduces the reliance on human intervention, increasing efficiency and ensuring quicker responses to incidents.
- **Scalability**: The system can easily scale, providing robust security solutions for a variety of settings, from small businesses to large cities.
- **Cost-Effectiveness**: AI-powered systems offer long-term cost savings by reducing the need for continuous human monitoring.
- **Enhanced Accuracy**: Deep learning algorithms reduce false positives and improve the accuracy of threat detection.
- **Privacy Assurance**: Strong data protection measures ensure that the system adheres to privacy laws, building public trust in AI surveillance applications.

## V. CONCLUSION

The development and deployment of AI-powered surveillance systems mark a transformative leap in modern security infrastructure. By enabling real-time monitoring, intelligent anomaly detection, and predictive threat analysis, these systems significantly enhance the ability to prevent and respond to potential security incidents proactively. Their integration introduces a new level of efficiency and precision far beyond the capabilities of traditional surveillance methods.

However, the adoption of such powerful technologies must be accompanied by a strong commitment to ethical responsibility. Critical issues such as data privacy, algorithmic bias, and the potential for misuse demand careful consideration. Upholding legal and regulatory standards, ensuring transparency in how AI models operate, and fostering public accountability are essential to maintain trust and prevent overreach.

As AI continues to evolve, sustained investment in research and development is vital—not only to improve system accuracy and reliability but also to build frameworks that balance innovation with human rights. Thoughtful implementation will determine whether AI surveillance becomes a tool for safety and progress or a source of societal concern.

The integration of biometric authentication, predictive analytics, and anomaly detection ensures that potential threats are identified early, reducing the risk of security breaches and improving response times. Furthermore, the system's ability to adapt to various environments and integrate with existing infrastructures makes it a flexible solution that can be applied across a range of security contexts, from urban surveillance to private enterprise.

Importantly, the system is designed with privacy and security in mind. Data encryption and compliance with global privacy regulations such as GDPR ensure that sensitive information is handled responsibly, addressing concerns about data misuse and public trust. The ongoing development and refinement of AI models within the system will continue to enhance its accuracy and efficiency, ultimately leading to more robust and reliable surveillance capabilities.

While the proposed system offers substantial benefits in terms of security, scalability, and automation, its success depends on continued research, development, and responsible implementation. As AI technology evolves, it is critical that ethical considerations remain at the forefront, ensuring that surveillance tools are used to protect public safety while respecting individual privacy and civil liberties.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405073|

Ultimately, this AI-powered surveillance system offers a transformative solution that not only improves security but also builds a foundation for smarter, safer urban environments. By combining advanced technology with responsible oversight, the system represents a step toward more secure, efficient, and trustworthy security infrastructure

## REFERENCES

[1].https://www.researchgate.net/publication/385009820_AIpowered_threat_detection_in _surveillance_systems_A_real-time_data_processing_framework
[2].https://www.researchgate.net/publication/387933428_AIpowered_surveillance_syste ms_and_anomaly_detection.
[3]. https://philarchive.org/archive/MOSAAE-2
[4]. https://arxiv.org/abs/2309.15084

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details