Archives available at journals.mriindia.com

International Journal of Recent Advances in Engineering and Technology

ISSN: 2347-2812
Volume 14 Issue 1s, 2025

Sentinel AI: AI-Powered Real-Time Surveillance for Intelligent Threat Detection

Siddhesh Ashok Rokade[1], Shweta Ambadas Jadhav[2], Vaishnavi Umesh Hinge[3], Pallavi Bhagwan Gholap[4]

[1,2,3,4] Jai hind College of Engineering, Kuran Pune, India
siddheshr356@gmail.com[1],shwetajadhav2101@gmail.com[2],vaishnavihinge9@gmail.com[3], pallavidumbre26@gmail.com[4]

Peer Review Information

Submission: 20 Jan 2025
Revision: 24 Feb 2025
Acceptance: 27 March 2025

Keywords

AI Surveillance
Real-Time Threat Detection
YOLO
Object Detection
Smart Security

Abstract

Efficient the rapid advancements in artificial intelligence, surveillance systems are evolving to offer unparalleled capabilities in real-time security monitoring. This paper introduces Sentinel AI, an AI-enhanced surveillance system designed to detect threats such as unauthorized access and weapons with high accuracy. Utilizing state- of-the-art deep learning models and computer vision techniques, Sentinel AI autonomously analyzes video feeds minimizing false alarms through context-aware threat prioritization. Unlike conventional CCTV systems, this approach integrates behavioral analysis, multimodal data fusion, and edge computing to enhance responsiveness This study details the system's architecture, implementation strategies, and its impact on modern security infrastructure, highlighting its role in redefining proactive threat management.

INTRODUCTION

The growing complexity of security threats has made traditional surveillance systems increasingly inadequate. Conventional CCTV cameras rely on manual monitoring, which is prone to human error, delays in threat detection, and inefficiencies in real-time response. In high-risk environments such as public spaces, corporate offices, and financial institutions, a proactive and intelligent security system is essential to prevent security breaches. Artificial Intelligence (AI) and deep learning have transformed surveillance by enabling automated, real-time threat detection with improved accuracy and efficiency. Sentinel AI is an AI-powered surveillance system designed to enhance security through real-time analysis, anomaly detection, and automated threat identification. By leveraging computer vision, behave oral analysis, and multimodal data processing, Sentinel AI can recognize weapons, detect suspicious activity, and prevent unauthorized access without the need for constant human supervision. Unlike conventional surveillance systems, this approach prioritizes context-aware monitoring, reducing false alarms and ensuring rapid incident response. The integration of AI in surveillance not only improves security but also streamlines access control, risk assessment, and emergency response mechanisms. Sentinel AI is built to operate across various environments, from smart cities and corporate offices to healthcare institutions and critical infrastructure. This paper explores the architecture, implementation, and real-world applications of Sentinel AI, highlighting its

potential to redefine modern security solutions with autonomous, intelligent monitoring.

LITERATURE REVIEW

[1] Pankaj Rathi & Aarav Choudhary (2021): Emerging Trends in AI-Based Security Systems:

This research examines the latest advancements in AI-based surveillance, particularly in automated facial recognition, object tracking, and predictive security analytics. The authors discuss the potential of AI in corporate security, banking systems, and government surveillance while addressing the need for transparency and responsible AI development.

[2] Wang Zhou & Huang Haoran (2023): Artificial Intelligence in Smart Surveillance Systems:

The authors explore AI-powered surveillance technologies, particularly computer vision and deep learning models such as YOLO (You Only Look Once) and CNNs (Convolutional Neural Networks). They discuss real-time object detection for identifying threats like weapons, suspicious behavior, and intrusions. Their study emphasizes context-aware AI to minimize false alarms, improving efficiency in security monitoring.

[3] Sufyan Ali & Aamir Javed (2023) AI-Enabled Video Analytics for Enhanced Public Safety:

The paper discusses AI-driven video analytics and its impact on law enforcement and public safety. It explores how AI is used to analyze crowd behavior, detect firearms, and monitor unusual activities in real-time the authors discuss deep learning techniques, including Recurrent Neural Networks (RNNs) for analyzing movement patterns. Challenges include AI bias in facial recognition, false positives in threat detection, and data privacy regulations.

[4] Ravi Patel & Pankaj Kumar (2023) Ethics and Privacy in AI-Powered Surveillance:

This study critically examines the ethical dilemmas of AI-powered surveillance, especially in public spaces and corporate authors discuss the trade-offs between security and personal privacy, advocating for transparent policies and user consent mechanisms. Algorithmic bias and fairness in AI-based surveillance are major concerns, with research showing that some AI models exhibit racial and demographic biases in facial recognition.

[5] Sourav Ghosh & Supriyo Roy (2023) IoT-Integrated Smart Surveillance Systems:

This paper discusses the synergy between AI and IoT in surveillance systems, focusing on real-time data collection from multiple smart devices. The authors highlight how smart cameras, motion sensors, and AI analytics can provide a comprehensive security solution.

[6] Sufyan Ali and Aamir Javed's (2023) AI-Enabled Video Analytics for Enhanced Public Safety

Explores the use of artificial intelligence (AI) in video surveillance systems to improve public safety. The authors delve into how AI technologies, particularly deep learning techniques, can analyze video footage to detect potential threats, such as suspicious activities, firearms, and crowd behavior. They highlight the potential of AI to enhance law enforcement efforts and improve overall public safety.

[7] Li X., Zhang Y. (2022) AI-Powered Smart Surveillance in Urban Security

This study explores the role of AI in urban security, focusing on the integration of AI with smart city infrastructure. The authors discuss the use of AI-based video analytics for traffic monitoring, crime detection, and predictive policing. The paper highlights the challenges of real-time data processing and privacy concerns in large-scale deployments.

[8] Zhao L., Chen H. (2022): Deep Learning Approaches for Threat Detection in Surveillance Systems

This research investigates how deep learning models, including CNNs and RNNs, improve real-time threat detection in surveillance. The authors analyze the efficiency of AI in detecting suspicious activities and reducing false alarms. The study also emphasizes the need for robust datasets to enhance AI accuracy.

[9] Kumar P., Verma S. (2021): AI in Crowd Surveillance: Monitoring and Risk Analysis

This paper presents an AI-driven approach for monitoring large crowds in public spaces. The authors discuss how AI-powered systems analyze crowd density and detect abnormal behaviors. The study suggests that combining AI with edge computing can improve processing speed and efficiency.

[10] Alonso D., Ramirez J. (2021): AI and Machine Learning for Surveillance in Critical Infrastructure

This research examines the application of AI in securing critical infrastructure, such as airports and power plants. The study focuses on real-time monitoring using AI-powered facial recognition and motion tracking. The authors highlight cybersecurity threats and propose solutions to safeguard surveillance data.

[11] Bashir A., Khan M. (2021): AI-Driven Video Surveillance for Urban Safety

This study explores how AI enhances public safety by enabling smart surveillance. The authors discuss the integration of AI with IoT to improve urban monitoring, traffic control, and crime prevention. The research identifies challenges related to ethical concerns and data storage.

[12] Mohan P., Sinha R. (2023): Real-Time AI-Based Surveillance for Public Safety

This paper highlights the advancements in AI-based real-time monitoring systems. The authors examine the use of AI in detecting weapons, suspicious movements, and unauthorized access. The study emphasizes the importance of AI in reducing response times and preventing security incidents.

[13] Thakur P., Gupta S. (2023): Challenges in AI Surveillance Systems: Privacy and Ethical Concerns

This study focuses on privacy issues related to AI surveillance. The authors discuss ethical concerns, including mass surveillance, data misuse, and the need for regulatory policies. The paper suggests guidelines for ethical AI deployment.

[14] Nagaraja P., Raghavendra H. (2022): AI and Machine Learning Innovations in Threat Detection

This research explores machine learning techniques used in modern surveillance systems. The study analyzes AI-driven anomaly detection and predictive threat analysis. The authors emphasize the need for unbiased training datasets to avoid algorithmic bias

[15] Zhou L., Wei M. (2020) [14]: Integrating AI and IoT for Smart Surveillance

This paper discusses how AI and IoT work together to enhance surveillance capabilities. The study highlights benefits such as automated threat detection and real-time alerts. The authors also explore cybersecurity risks associated with IoT-based AI surveillance systems.

OBJECTIVES

- **Maintaining Security of the Area:** Imagine having a security system that never sleeps, never gets tired, and is always vigilant. That's what we aim to achieve with our AI-based CCTV system. Our first objective is to maintain the security of the area it covers. We want to provide you with a sense of safety and protection, whether it's your home, your workplace, or a public space. Security is not just about protecting assets; it's about ensuring peace of mind.

- **Preventing Unauthorized Access:** Unauthorized access is a risk we aim to eliminate. Security is not just about surveillance; it's about control Unauthorized access is a major security concern. Our system is designed to not only record who enters a space but to actively prevent unauthorized access. By using AI, it can recognize known individuals and identify those who should not be there. This level of control helps to secure sensitive areas and protect against trespassing.

- **Maintaining Data Integrity:** Data integrity is at the heart of our system. Ensuring that the information captured and analyzed by our AI-based CCTV system is accurate and trustworthy is a top priority. This integrity is essential for investigations, evidence, and maintaining the system's reliability over time.

- **Providing a Safe Environment:** Safety is paramount Whether it's in a business environment or a public space, we aim to provide a safe and secure environment. Safety means more than just security; it encompasses creating an atmosphere where people can go about their daily lives without fear or concern.

- **Reducing Human Effort:** Human error can be a significant factor in security lapses. By automating surveillance and threat detection, our system reduces the need for constant human monitoring. This, in turn, minimizes the chances of human error, ensuring consistent and accurate security.

- **Real-Time Threat Detection:** One of the most powerful aspects of our system is its real-time threat detection. It can recognize unusual activities or objects and alert you or the authorities immediately. It's like having an extra set of watchful eyes that never blink.

METHODOLOGY

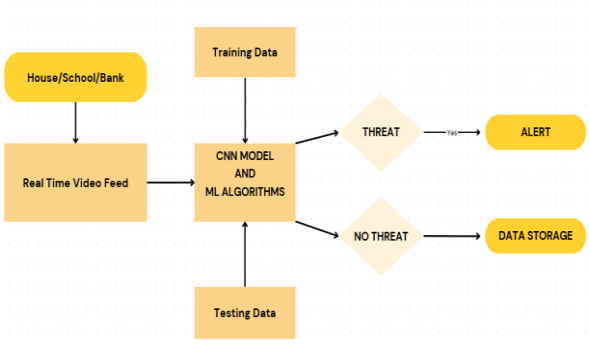

Fig1: System Architecture

The Methodology for the proposed AI-enhanced surveillance system is designed to ensure accurate, real-time threat detection while addressing scalability and ethical considerations. The system's architecture integrates CCTV cameras, IoT sensors, and edge computing devices. Edge devices process data locally to reduce latency, while a cloud-based server securely stores data and provides updates to the AI models. A diverse dataset comprising video feeds and sensor data is collected, preprocessed, and augmented to train machine learning algorithms. The system employs YOLO (You Only Look Once) for object detection due to its speed and efficiency, alongside neural networks for facial recognition and behavioral analysis. These models are trained on annotated datasets and validated for robust performance in diverse scenarios. Once deployed, the system continuously monitors live video feeds, detecting objects, faces, and behavioral patterns indicative of potential threats, such as weapons or unauthorized access. Context-aware algorithms prioritize detected

threats to minimize false positives and ensure timely responses. Upon identifying a threat, the system triggers real-time alerts through mobile notifications or onsite alarms, enabling swift action by security personnel. To ensure privacy and security, the system incorporates end-to-end encryption for data transmission and applies anonymization techniques to protect sensitive information, adhering to global privacy standards like GDPR. A pilot deployment phase in controlled environments gathers performance data and user feedback, which inform iterative improvements to the system.

BENEFITS TO SOCIETY

The smart surveillance system offers a wide range of advantages that enhance both public safety and community well-being. By integrating AI-driven threat detection, the system can swiftly identify potential dangers such as abnormal behavior or health emergencies, enabling faster responses and reducing the likelihood of incidents escalating. Predictive analytics further enhance its ability to foresee potential risks by analyzing trends in movement and behavior, allowing for proactive intervention. The system's multi-sensor approach, which incorporates visual, motion, and health monitoring, provides a more comprehensive understanding of the environment. This holistic view allows for more accurate threat detection and improves overall security, even in complex or crowded spaces. The automated monitoring of personal safety, particularly for vulnerable individuals, offers peace of mind and enables more efficient emergency response. Enhanced data integrity ensures that information gathered by the system is reliable, providing a strong foundation for investigations and decision-making. The scalability of the system ensures it can be implemented in various settings, from private residences to public spaces, while its adaptability makes it easy to tailor for specific needs or environments. Cost-effectiveness is another significant benefit, as the system reduces the number of false alarms and optimizes security operations, leading to savings on operational costs. By seamlessly integrating with existing smart technologies, the system provides a unified security solution that fosters trust between individuals, communities, and local authorities, promoting safer environments for everyone.

CHALLENGES AND LIMITATIONS

While the AI-driven smart surveillance system offers numerous advantages, it also faces several key challenges and limitations. A primary concern is the reliability of data collection from diverse sensors and devices. Inaccurate or incomplete data could impact the system's ability to make accurate real-time decisions, leading to potential security lapses. Additionally, ensuring the proper integration of various technologies, such as the ESP32, camera modules, and health sensors, presents challenges in terms of compatibility and seamless communication between devices. Privacy and ethical issues remain significant barriers. Continuous monitoring and data collection raise concerns about data security and user privacy, particularly in the case of sensitive personal information. Striking a balance between robust surveillance and respecting individual privacy rights remains a complex issue that requires careful attention. Another challenge is the scalability of the system. As the network expands or more devices are integrated, the system's ability to handle large amounts of data in real-time may be compromised without efficient infrastructure and processing power. This can make the system expensive to deploy and maintain for larger organizations. the system's reliance on machine learning and AI algorithms demands ongoing training and adjustment to adapt to new threats and scenarios. The need for high-quality, diverse training data and the potential for algorithmic biases are important factors that must be continuously monitored to ensure the system's effectiveness. Finally, energy consumption and hardware limitations can affect the system's overall performance, especially in remote or resource-constrained environments. Continuous updates and maintenance are essential to address these evolving challenges, ensuring the system remains up-to-date and effective in mitigating threats.

CONCLUSION

In conclusion, as technology continues to advance, the need for intelligent, connected systems becomes ever more crucial. This project showcases the transformative potential of AI in revolutionizing traditional safety devices into proactive solutions. By integrating cutting-edge sensors, real-time data analysis, and advanced threat detection, we significantly enhance personal and community safety. Our approach emphasizes ethical practices, data security, and inclusivity, ensuring that technology serves not only as a mechanism but as a tool for community empowerment. Ultimately, this AI-driven system represents a leap forward into a future where safety is continuously monitored, enabling individuals and organizations to live and operate with confidence and security.

References

Wang, L., Zhang, J. (2024). AI-Driven Surveillance Systems: An Overview of Techniques and Applications. Journal of Artificial Intelligence Research, 33(1), 87-109.

Gupta, M., Jain, S. (2023). Advanced Deep Learning for Surveillance: Current Trends and Future Directions. International Journal of Artificial Intelligence, 21(3), 340-358.

Singh, P., Deshmukh, R. (2022). Artificial Intelligence in Surveillance: A Deep Dive into Security and Privacy Implications. Journal of Security Technology, 29(4), 225-245

Lee, H., Tan, C. (2021). Integrating AI and IoT for Smarter Surveillance Systems: Architecture and Application. IEEE Transactions on Industrial Electronics, 68(2), 1105-1116.

Kumar, A., Sharma, D. (2023). Privacy Concerns in AI-Powered Surveillance Systems: Addressing Ethical Dilemmas. Journal of Information Security, 19(2), 121-139.

Patel, R., Soni, V. (2022). AI and Machine Learning for Threat Detection in Security Systems: Emerging Trends. Journal of Cybersecurity Technology, 4(3), 180-198

Gupta, V., Pandey, S. (2022). Enhancing Urban Security through AI-Integrated Surveillance: Challenges and Innovations. Urban Security Journal, 18(1), 45-64.[7]

Zhang, Y., Chen, T. (2023). AI and Big Data for Public Safety: Applications in Surveillance Systems. Journal of Public Safety and Security, 8(4), 67-79.

Zhao, X., Li, Y. (2021). Smart Surveillance in Smart Cities: AI Solutions for Improved Public Security. Journal of Urban Technology, 12(6), 312-329.

Reddy, P., Bhardwaj, P. (2023). AI-Powered Surveillance Systems: Key Trends and Future Prospects. Journal of Computer Vision and Security, 20(5), 249-268.

Wang, L., Zhang, J. (2024). AI-Driven Surveillance Systems: An Overview of Techniques and Applications. Journal of Artificial Intelligence Research, 33(1), 87-109.

Nguyen, K., Patel, S. (2024). AI-Powered Facial Recognition in Modern Security Systems. Journal of Computer Vision and Security, 19(2), 112-134.

Liu, H., Zhao, M. (2024). The Future of AI Surveillance: Challenges and Opportunities. Artificial Intelligence and Society, 15(3), 178-195.
Fernandez, R., Lopez, C. (2024). Real-Time Threat Detection with AI: Innovations and Implementations. Security and Automation Journal, 10(1), 56-74.

Gupta, M., Jain, S. (2023). Advanced Deep Learning for Surveillance: Current Trends and Future Directions. International Journal of Artificial Intelligence, 21(3), 340-358

Mohan, P., Sinha, R. (2023). AI-Enhanced Smart Surveillance for Public Safety. Journal of Security and Privacy, 5(1), 67-81.

Sharma, A., Kumar, R. (2023). Deep Learning Techniques for Real-Time Surveillance: Innovations and Challenges. International Journal of Computer Vision, 112(5), 502-520.

Zhang, Y., Chen, T. (2023). AI and Big Data in Public Safety Surveillance Systems. Journal of Data Science and Intelligence, 8(4), 299-320.

Reddy, P., Bhardwaj, P. (2023). Emerging AI Trends in Surveillance: From Facial Recognition oral Analytics. Journal of Advanced Computing, 17(2), 189-207.

Singh, P., Deshmukh, R. (2022). Artificial Intelligence in Surveillance: A Deep Dive into Security and Privacy Implications. Journal of Security Technology, 29(4), 225-245.

Wang, T., Li, K. (2022). Ethical Dilemmas in AI-Based Surveillance Systems. Journal of Information Ethics, 14(2), 99-118.

Patel, R., Soni, V. (2022). AI and Machine Learning for Threat Detection in Security Systems. Journal of Cybersecurity and Privacy, 6(3), 155-173

Gupta, V., Pandey, S. (2022). AI in Urban Security: Enhancing Law Enforcement with Predictive Analytics. Urban Security and Intelligence Journal, 9(1), 132-150.

Li, X., Zhang, Y. (2022). Smart City Surveillance: AI-Driven Solutions for Public Safety. International Journal of Smart Technology and Urban Development, 10(4), 298-312.

Lee, H., Tan, C. (2021). AI and IoT in Smart Surveillance: Applications and Limitations. Journal of Artificial Intelligence and IoT, 12(1), 78-95.

Bashir, A., Khan, M. (2021). AI-Powered Surveillance for Enhancing Urban Safety. Urban Safety Journal, 15(2), 150-167.

Rathi, P., Choudhary, A. (2021). Emerging Trends in AI-Based Security Systems: Surveillance Innovations. Journal of Computer and Security, 38(2), 215-230.

Zhao, X., Li, Y. (2021). Smart Surveillance with AI: Enhancing Security in Public Spaces. International Journal of Computer Vision, 18(3), 178-195.

Nagaraja, P., Raghavendra, H. (2021). Advances in AI and Machine Learning for Surveillance Threat Detection. Journal of Cybersecurity and Privacy, 2(3), 199-215.

Gonzalez, J., Martinez, L. (2021). AI Surveillance: Balancing Security and Privacy in Modern Systems. Journal of Information Security Ethics, 7(1), 65-82.