International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 11 | Nov 2025 www.irjet.net p-ISSN: 2395-0072

Artificial Intelligence Based Surveillance Systems: A Survey, Challenges and Future Trends

Abdullah Al-Atwi[1,*], Fayez Alkhaibari[1], Khalid Al-Malki[1], Yasser Al-Juhani[1], Hasan Shtiewi[1]

[1.] *College of Computing, Fahad Bin Sultan University, Saudi Arabia*
**(Corresponding Author)*

Abstract – *AI-based surveillance systems leverage computer vision, machine learning, and IoT sensors to enable real-time monitoring, intelligent analysis, and automated threat response, enhancing security and operational efficiency in smart cities and public spaces. However, their successful implementation hinges on addressing critical cybersecurity and privacy challenges, including secure development frameworks and ethical handling of sensitive data like location information and medical records. This work analyzes these dual imperatives, providing researchers with insights to develop more secure and privacy-preserving surveillance solutions, ultimately fostering trustworthy smart city ecosystems that balance technological advancement with fundamental rights protection.*

Key Words: **Surveillance, Security, Privacy, Agents, Medical Records.**

1. INTRODUCTION

AI-based surveillance systems use computer vision, machine learning, and IoT sensors to automatically monitor, analyze, and respond to activities in real time. These systems enhance security, automate threat detection, and improve operational efficiency in smart cities, businesses, and public spaces [1].

1.2 Framework of AI-Based Surveillance Systems

A typical AI surveillance system follows a pipeline that consists of five stages [2], as described below:

1. **Data Acquisition**
   - Sources: CCTV cameras, drones, IoT sensors, facial recognition scanners, license plate readers.
   - Data Types: Video feeds, thermal imaging, audio, motion detection signals.
2. **Preprocessing**
   - Noise reduction (e.g., stabilizing shaky footage).
   - Frame extraction (converting video into analyzable images).
3. **AI Processing & Analysis**
   - Object Detection (YOLO, Faster R-CNN).
   - Facial Recognition (DeepFace, ArcFace).
   - Behavioral Analysis (anomaly detection using LSTM networks).
4. **Decision-Making**
   - Real-time alerts (e.g., gun detection, unauthorized access).
   - Automated responses (e.g., locking doors, notifying authorities).
5. **Storage & Retrieval**
   - Cloud/edge storage for forensic analysis.
   - Indexed databases for fast search (e.g., finding a suspect across multiple cameras).

1.2 Key Components of AI-Based Surveillance Systems

In terms of components, an AI-based surveillance system consists of five components that are integrated together to achieve the goal, where the input of a given component will be used as output to the next component [2]. Table 1 summarizes the components.

Table -1: Key Components of AI-based Surveillance Systems.

Component	Function
Cameras & Sensors	Capture visual/audio data
Edge Devices	Process data locally (low latency)
AI Models	Analyze data for threats
Cloud/Server	Store & analyze bulk data
User Interface	Monitor & control the system

Each component uses different technologies enabling it to achieve its function. They are as follows:

1. Cameras & Sensors: IP cameras, LiDAR, thermal imaging.
2. Edge Devices: NVIDIA Jetson, Raspberry Pi + AI accelerators.
3. AI Models: YOLOv8, OpenPose, DeepSORT.
4. Cloud/Server: AWS Rekognition, Azure AI.
5. User Interface: Dashboards (e.g., Milestone XProtect).

1.3 Applications in Smart Cities

AI-based surveillance systems are widely used in smart cities to facilitate daily activities related to detect malicious actions or for facilitating monitoring governmental process [3]. Below is a list of applications supported with real world examples.

1. **Public Safety**
   - Gun/weapon detection in crowds.
   - Missing person tracking via facial recognition.
2. **Traffic Management**
   - Automatic license plate recognition (ALPR) for tolls/parking.
   - Congestion analysis using vehicle flow tracking.
3. **Retail & Fraud Prevention**
   - Shoplifting detection via pose estimation.
   - Queue monitoring to optimize staff allocation.
4. **Industrial Security**
   - Intrusion detection in restricted areas.
   - Worker safety compliance (e.g., helmet detection).
5. **Healthcare**
   - Fall detection for elderly care.
   - Crowd density monitoring in hospitals.

2. Related Works: Systematic Review

This section provides a review related to some AI-based surveillance systems. In general, AI-based surveillance systems are classified into four categories, as summarized in Table 2.

Table -2: Taxonomy of some AI-based Surveillance Systems.

System Name	Key Features	Applications
Smart Home System	Face recognition, voice control, fire and gas leak detection, remote control	Home automation, security, and convenience
Hawk-Eye Threat Detector	Real-time threat detection, motion detection, multi-class classification	Public surveillance in schools, malls, and high-security areas
AI-Powered Smart Camera	Long-range communication, object and face recognition, secure data transmission	Home and car security, industrial monitoring
Smart-Watcher	Real-time object detection, motion detection, mobile app alerts	Security for small to medium-scale premises

Authors of work [4] proposed an intelligent embedded video monitoring system for home surveillance using IoT and computer vision techniques. The system integrates a motion detection algorithm with video recording and alert mechanisms. It employs Raspberry Pi as the central controller interfaced with a digital camera, capturing video at a resolution of 640x480 at 24 fps. Their approach includes erosion and dilation processing to fine-tune motion detection and reduce noise. Human detection is prioritized only after movement is initially sensed, which saves processing power and ensures important events are recorded. The system achieved around 80% accuracy in recognizing human forms, although performance decreased with multiple subjects. The implementation also supports cloud storage and remote access, with SMS and email alerts enhancing its practical usability. The results indicate reliability and efficiency, making it suitable for real-time home monitoring applications, with potential for extension to outdoor or border surveillance.

Authors of work [5] developed a smart IoT-based multi-camera surveillance system emphasizing affordability and modular flexibility. Unlike proprietary systems with expensive SDKs, their solution uses open-source image processing methods and supports multiple camera inputs. The system allows users to customize video analytics modules, improving adaptability across various surveillance setups. Methodologically, user feedback was the primary form of evaluation. A usability survey with 10 participants indicated high awareness of CCTV systems and general satisfaction with the additional on-screen video details. 90% of users found the system usable, and 95% regarded it as more affordable than existing commercial options. Although some users found additional features distracting, the option to add new modules was generally well-received. The system provides a strong base for enhancing existing camera infrastructures, especially for individuals or organizations with limited budgets.

Authors of work [6] introduced an intelligent video surveillance analysis service built on a Platform-as-a-Service (PaaS) architecture for large-scale cloud-based deployment. Their system, part of the CityEyes project, integrates more than 25,000 surveillance devices across a metropolitan area. Key components include a license plate recognition engine, camera health monitoring, and network video recorder (NVR)/digital video recorder (DVR) integration. The methodology involves centralized data processing and storage in the cloud, enabling real-time analytics and rapid incident detection. The system's effectiveness was validated through its application in actual criminal investigations, where it reduced the manpower needed for reviewing video data. Results confirmed improved usability and efficiency, suggesting that cloud-based services can significantly enhance traditional surveillance operations. Their approach also demonstrates scalability, making it a candidate model for future intelligent surveillance infrastructures.

Authors of work [7] proposed a public surveillance system that combines anomaly detection and weapon detection using a deep learning approach. The system incorporates Long-term Recurrent Convolutional Networks (LRCN) for identifying abnormal events (e.g., fights, explosions) and YOLO for detecting visible weapons. Their method emphasizes the importance of temporal modeling in surveillance and achieves around 79% accuracy for anomaly detection. Furthermore, they use MongoDB GridFS for efficient video storage and implement a GUI for monitoring. The framework supports both crowd density estimation and weapon detection in real-time, making it suitable for deployment in smart cities. While the architecture is innovative, especially in combining LRCN with YOLO. The lower performance may stem from the diversity and complexity of anomalies as opposed to specific object detection.

Authors of work [8] proposed a layered software architecture tailored for third-generation mobile distributed video surveillance (MDSV) systems. The architecture is split into two tiers: the vigilant tier for low-resource mobile devices and the analyst tier for high-capacity systems like PCs. Each tier comprises specialized layers handling communication, sensing, alerting, and processing. A prototype was developed and tested, showing the architecture supports key surveillance functionalities such as protection, detection, and response while operating efficiently even in resource-constrained environments. The architecture also provides developers with a structured guideline for building robust MDSV systems. Future plans include incorporating computer vision for action and object recognition.

Authors of work [9] developed an innovative IoT-based surveillance system that integrates smart cameras with chatbot functionality through platforms like Telegram and WhatsApp. The system employs computer vision algorithms to continuously monitor environments, detect suspicious activities, and provide real-time alerts to users through conversational interfaces. This approach enables homeowners and security personnel to remotely access live footage and receive instant notifications about potential threats. The solution addresses the limitations of traditional surveillance systems by offering two-way communication, automated threat detection, and user-friendly interaction at a reduced operational cost. While effective for domestic and small-scale commercial applications, the authors suggest future enhancements could incorporate advanced facial recognition and deeper integration with smart home automation systems to expand its capabilities.

Authors of work [10] developed an IoT-based smart doorbell system using Raspberry Pi, PIR motion sensors, and a camera module to enhance home security. The system automatically detects visitors through motion sensing, captures their images, and sends real-time notifications with photos to the homeowner's email and mobile device. Experimental results demonstrated successful intruder detection, though the accuracy depended on proper sensor alignment and camera positioning. The researchers implemented the system using Python programming for GPIO connectivity and sensor integration, creating a cost-effective solution that allows remote monitoring via internet connectivity. While currently focused on basic motion detection and image capture, the authors suggest future enhancements could incorporate computer vision and AI for advanced features like facial recognition and gesture identification to further improve security capabilities.

Authors of work [11] created an AI-powered weapon detection system for surveillance videos using TensorFlow framework, aiming to automate threat identification in public spaces. Their solution analyzes video footage to recognize five categories of firearms (handguns, shotguns, automatic rifles, sniper rifles, and submachine guns) with precision levels of 0.8524 (IoU=0.50) and 0.7006 (IoU=0.75). The system employs key frame extraction with optimal window sizing to balance processing efficiency and detection accuracy, demonstrating improved performance through training iterations that reduced classification and localization losses. While effective for weapon identification, the researchers acknowledge the need for expanded training datasets and propose developing dual operation modes (energy-saving for low-traffic areas and high-performance for crowded spaces) to enhance practical implementation in various security scenarios.

3. Cybersecurity-Based Analysis

AI-based surveillance systems can be analyzed from two main aspects, which are security and privacy. The analyzing leads to extract challenges and future trends.

3.1 Security Based Analysis

AI-based surveillance systems use agent based technology as an infrastructure to develop real systems that contribute to solve problems. Using agents (both stationary and mobile ones) arise many security issues. Authors of [12] presented a systematic review related to the security of agents. They presented security requirements, protection goals, and attacks that may be occurred and negatively affect agents. The issues mentioned in their work should be considered during building agent based systems. in responding to such issues, authors of [13] presented a dummy based method to protect agents against host machines when act as an attacker. In same context, authors of [14] proposed a self protection approach for agents that serve mobile cars in order to ensure secure information exchange. In regards to web security, collaboration based method is introduced in [15]. The key idea is to enable surveillance systems to take into consideration security issues arisen during collaboration in terms of data exchanging. It is noticed that agent based systems deal with big data within smart cities. Here, manipulating big data

requires special techniques such as data mining, text mining, and web mining [16]. Security issues related to such technologies should be considered to strengthen level of protection.

In conclusion, AI-based surveillance systems depend heavily on agent software technology, and many security issues open door to various vulnerabilities, security gaps, and threats. Such issues may negatively affect security of AI-based surveillance systems.

3.2 Privacy Based Analysis

Many AI-based surveillance systems use location based services as primary way to facilitate daily activities of individuals within smart cities. Privacy issue is a big concern that may lead to serious problems if protection of personal data is ignored. In the context of privacy protection, work [17] provided an approach to protect Knn queries used to monitor and retrieve points of interests that users search. Fragmentation method is utilized to strengthen level of privacy so that attackers can mot obtain sensitive information about users. In the same context, work [18] introduced an AES based approach that harnesses dummies to protect users' privacy against servers. Such approaches are taken from a survey provided in [19], where researchers detailed various privacy protection approaches and their related limitations. In terms of hiding within crowds, a leader based method is proposed in [20]. The key idea is to mask activities against monitoring by exploiting random motion of monitored entities. This leads to strengthen level of privacy in AI-based surveillance systems, but still suffer form the fact that the leader can act as a malicious party even mutual benefit is used. Work [21] employed deep learning techniques to develop privacy protection system. CNN is used and can be used to strengthen AI-based surveillance systems. However, privacy of training data may be attacked. Work [22] addressed the problem of achieving load balancing between power consumption and privacy protection level. This is an important aspect in AI-based surveillance systems in terms of complexity and computational resources.

In medical domain, AI-based surveillance systems play important role, but privacy of medical data is critical. In terms of privacy, medical records of patients must not be revealed. AI-based surveillance systems developers must take responsibility related to protect patients' data when using deep learning techniques. In work [23] breast cancer diagnostic system is proposed using enhanced convolutional neural networks, where privacy is protected by removing IDs and names of patients. Similarly, the work [24] proposed lung cancer detection system, and here privacy is ensured by masking sensitive information attached with medical images. During COVID-19 epidemic, research society made a race for developing diagnostic intelligent systems to detect this virus and its series. Work [25] proposed medical system to detect covide-19 using advanced deep learning technique supported by an augmentation method. Applying augmentation on medical images may reveal personal information about training medical records. Privacy is ensured by using obfuscation technique that depends on replacing personal information by a range of data. The key idea is derived from a survey provided in work [26].

4. Challenges and Future Trends

Based on the analysing provided in previous sections, cybersecurity based challenges can be summarized in tow points as follows:

1. When developing AI-based surveillance systems using agents, security of agents must be ensured. Otherwise, the system will crash as the agents are responsible for performing tasks. When tasks are modified, the results will be poisoned.
2. When developing AI-based surveillance systems using location based services, privacy must be ensured as attackers may track locations of users or analysing the issued queries. Otherwise, a malicious profile can be created about victims (users).
3. When developing AI-based surveillance systems in medical domain, sensitive data of patients must be protected. Otherwise, medical companies will undergo penalties according to laws.

Future trends in AI-based surveillance systems are inspire from the challenges mentioned above, which are:

1. Developing novel controls to protect agents.
2. Developing novel controls to protect privacy.

5. CONCLUSION

Security and privacy in AI-based surveillance systems are critical for success of such system in reality. This work provided analysing of the tow aspects of cybersecurity. Analysing includes agents used to develop AI-based surveillance systems as well as privacy when using location based services and handling medical records. This work helps researchers to focus of security and privacy aspects in their future works. When both security and privacy are ensured in AI-based surveillance systems, smart cities will be foster.

REFERENCES

[1] Villegas-Ch, William, Joselin García-Ortiz, and Santiago Sánchez-Viteri. "Toward intelligent monitoring in IoT: AI applications for real-time analysis and prediction." IEEE Access 12 (2024): 40368-40386.

[2] Dsouza, Arnold, et al. "Artificial intelligence surveillance system." 2022 International Conference on Computing,

Communication, Security and Intelligent Systems (IC3SIS). IEEE, 2022.

[3] Luckey, Daniel, et al. "Artificial intelligence techniques for smart city applications." International Conference on Computing in Civil and Building Engineering. Cham: Springer International Publishing, 2020.

[4] Virendra, V. Shete and N. Ukunde, "Intelligent embedded video monitoring system for home surveillance," 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2016, pp. 1-4, doi: 10.1109/INVENTIVE.2016.7823191.

[5] H. Razalli, M. H. Alkawaz and A. S. Suhemi, "Smart IOT Surveillance Multi-Camera Monitoring System," 2019 IEEE 7th Conference on Systems, Process and Control (ICSPC), Melaka, Malaysia, 2019, pp. 167-171, doi: 10.1109/ICSPC47137.2019.9067984.

[6] T. -S. Chen, M. -F. Lin, T. -c. Chieuh, C. -H. Chang and W. -H. Tai, "An intelligent surveillance video analysis service in cloud environment," 2015 International Carnahan Conference on Security Technology (ICCST), Taipei, Taiwan, 2015, pp. 1-6, doi: 10.1109/CCST.2015.7389648.

[7] P. Joglekar, D. Jha, P. Dhorage, D. Thakkar and O. Dhumal, "Intelligent Public Surveillance System," 2025 3rd International Conference on Intelligent Systems, Advanced Computing and Communication (ISACC), Silchar, India, 2025, pp. 323-328, doi: 10.1109/ISACC65211.2025.10969367.

[8] Y. Viveros Martínez, E. López Domínguez, Y. Hernández Velázquez, S. Domínguez Isidro, M. A. Medina Nieto and J. De La Calleja, "Layered Software Architecture for the Development of Third-Generation Video Surveillance Systems," in IEEE Access, vol. 7, pp. 98507-98521, 2019, doi: 10.1109/ACCESS.2019.2930401

[9] G. S, A. R, P. B, K. A, V. V. A and L. K, "Design and Development of IoT Camera with CHATBOT for Domestic Surveillance," 2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS), Chennai, India, 2023, pp. 1-5, doi: 10.1109/ICCEBS58601.2023.10448981.

[10] S. Akter, R. A. Sima, M. S. Ullah and S. A. Hossain, "Smart Security Surveillance using IoT," 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2018, pp. 659-663, doi: 10.1109/ICRITO.2018.8748703.

[11] S. Xu and K. Hung, "Development of an AI-based System for Automatic Detection and Recognition of Weapons in Surveillance Videos," 2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE), Malaysia, 2020, pp. 48-52, doi: 10.1109/ISCAIE47305.2020.9108816.

[12] Bandar Alluhaybi, Mohamad Shady Alrahhal, Ahmed Alzhrani and Vijey Thayananthan. “A Survey: Agent-based Software Technology Under the Eyes of Cyber Security, Security Controls, Attacks and Challenges”. International Journal of Advanced Computer Science and Applications (IJACSA) 10.8 (2019). http://dx.doi.org/10.14569/IJACSA.2019.0100828

[13] Alluhaybi, Bandar, et al. "Dummy-based approach for protecting mobile agents against malicious destination machines." IEEE Access 8 (2020): 129320-129337.

[14] Alluhaybi, Bandar, et al. "Achieving self-protection and self-communication features for security of agentbased systems." (2020).

[15] Albarrk, Majed Abdullah, and Mohamad Shady Alrahhal. "Web Applications Security: More Collaboration." (2020).

[16] Alrahhal, Mohamad Shady, and Adnan Abi Sen. "Data mining, big data, and artificial intelligence: An overview, challenges, and research questions." (2018).

[17] Mohamad Shady Alrahhal, Maher Khemakhem and Kamal Jambi. “Agent-Based System for Efficient kNN Query Processing with Comprehensive Privacy Protection”. International Journal of Advanced Computer Science and Applications (IJACSA) 9.1 (2018). http://dx.doi.org/10.14569/IJACSA.2018.090108

[18] Mohamad Shady Alrahhal, Muhammad Usman Ashraf, Adnan Abesen and Sabah Arif. “AES-Route Server Model for Location based Services in Road Networks”. International Journal of Advanced Computer Science and Applications (IJACSA) 8.8 (2017). http://dx.doi.org/10.14569/IJACSA.2017.080847

[19] Alrahhal, Mohamad Shady, Maher Khemakhem, and Kamal Jambi. "A SURVEY ON PRIVACY OF LOCATION-BASED SERVICES: CLASSIFICATION, INFERENCE ATTACKS, AND CHALLENGES." Journal of Theoretical & Applied Information Technology 95.24 (2017).

[20] Alrahhal, Hosam, et al. "A symbiotic relationship based leader approach for privacy protection in location based services." ISPRS International Journal of Geo-Information 9.6 (2020): 408.

[21] Abdullah S. Alyousef, Karthik Srinivasan, Mohamad Shady Alrahhal, Majdah Alshammari and Mousa Al-Akhras. “Preserving Location Privacy in the IoT against Advanced Attacks using Deep Learning”. International Journal of Advanced Computer Science and Applications (IJACSA) 13.1 (2022). http://dx.doi.org/10.14569/IJACSA.2022.0130152

[22] Alrahhal, Mohamad Shady, Maher Khemekhem, and Kamal Jambi. "Achieving load balancing between privacy protection level and power consumption in location based services." International Research Journal of Engineering and Technology 5.3 (2018): 619-625.

[23] Mona Alfifi, Mohamad Shady Alrahhal, Samir Bataineh and Mohammad Mezher. "Enhanced Artificial Intelligence System for Diagnosing and Predicting Breast Cancer using Deep Learning". International Journal of Advanced Computer Science and Applications (IJACSA) 11.7 (2020). http://dx.doi.org/10.14569/IJACSA.2020.0110763

[24] Alrahhal, Mohamad Shady, and Eftkhar Alqhtani. "Deep learning-based system for detection of lung cancer using fusion of features." International Journal of Computer Science & Mobile Computing 10.2 (2021): 57-67.

[25] Mohamad Shady Alrahhal, Mohammad A. Mezher, Osamah A.M. Ghaleb, Mohammad Al-Hjouj, Raghad Sehly and Samir Bataineh. "An Augmentation-Based System for Diagnosing COVID-19 Using Deep Learning". International Journal of Advanced Computer Science and Applications (IJACSA) 16.8 (2025). http://dx.doi.org/10.14569/IJACSA.2025.0160819.

[26] Alrahhal, Mohamad Shady, and Majed Abdullah Albarrk. "A Survey of the COVID-19 Epidemic Through the Eyes of Artificial Intelligence and Deep Learning: Challenges and Research Questions." (2020).