ISSN: 2455 - 9172

EIJO Journal of Engineering, Technology And Innovative Research (EIJO–JETIR)

Einstein International Journal Organization (EIJO)

Available Online at: www.eijo.in

Volume – 10, Issue –2 , March - April - 2025 , Page No. : 01 - 06

AI For smart Surveillance and Anomaly Detection

[1]Pawan Sen, HOD, Department of Computer Science, Arya College of Engineering, Jaipur

[2]Digvijay Singh Rathore, Research Scholar, Department of Computer Science, Arya College of Engineering, Jaipur.

[3]Aradhya Gupta, Research Scholar, Department of Computer Science, Arya College of Engineering, Jaipur.

Abstract

As customer service rapidly evolves in the digital era, businesses are increasingly deploying chatbots to manage user interactions, aiming to reduce costs, increase efficiency, and provide instant support. At the same time, human agents continue to play a vital role in delivering personalized, empathetic, and adaptive communication. This research paper presents a comparative study of chatbots and human agents, examining their respective strengths and limitations across key factors such as response time, emotional intelligence, scalability, cost-effectiveness, problem-solving capability, and customer satisfaction. Drawing on real-world implementations, user behavior analysis, and industry practices, the study reveals that while chatbots offer superior speed, availability, and consistency, they struggle with complex queries and emotional nuance—areas where human agents excel. The paper argues that the most effective customer service models are hybrid systems that leverage the efficiency of AI-powered chatbots alongside the emotional intelligence and adaptability of human support. As AI technologies continue to advance, understanding the appropriate use cases for automation versus human interaction becomes crucial for businesses seeking to enhance customer experience while maintaining operational efficiency

Keywords: Chatbots, Human Agents, Customer Support, Artificial Intelligence, Natural Language Processing, Customer Experience, Conversational AI.

Introduction

The increasing demand for public safety and asset protection has led to rapid advancements in surveillance systems. Traditional surveillance methods, dependent on human operators, are limited by attention span and scalability. The integration of Artificial Intelligence (AI) with surveillance technology introduces smart surveillance systems capable of automating threat detection, reducing human error, and enhancing real-time decision-making.

Smart surveillance systems powered by AI leverage computer vision, deep learning, and pattern recognition to analyze video feeds and detect anomalies such as unusual movements, unauthorized access, crowding, or violence. These systems find applications in airports, shopping malls, transportation networks, military zones, and even residential areas.

A key challenge addressed by AI-based surveillance is anomaly detection — identifying behavior or patterns that deviate from the norm. Unlike predefined rule-based systems, AI models can learn what constitutes "normal" behavior in a particular environment and automatically flag deviations, thereby improving both reactive and proactive security.

The integration of edge computing further empowers smart surveillance by enabling real-time analysis at the source, reducing latency, bandwidth usage, and enabling quick responses. In parallel, advancements in neural networks, such as

Convolutional Neural Networks (CNNs) for object detection and Recurrent Neural Networks (RNNs) for behavioral sequence modeling, have substantially boosted system performance.

This paper explores the technical framework, methodologies, datasets, and challenges in developing AI-powered surveillance systems focused on anomaly detection. We evaluate how machine learning algorithms are applied to live and recorded footage, the role of unsupervised and semi-supervised learning, and how these models adapt to dynamic environments.

Figure 1

System Architecture and Workflow

A typical AI-powered smart surveillance system comprises several key components designed to work together in real time. The overall architecture involves data capture, preprocessing, feature extraction, model inference, and alert generation. Each component plays a vital role in ensuring that the system remains accurate, efficient, and responsive.

1. Video Input Layer

This layer involves collecting live video feeds through IP cameras, CCTV, or drone-based systems. These feeds are either stored in the cloud or streamed directly to edge devices for real-time processing.

2. Preprocessing Layer

Raw video data is often noisy and requires preprocessing. Tasks include frame extraction, resolution adjustment, background subtraction, object detection (using YOLO, SSD, or Faster R-CNN), and removal of redundant frames. Preprocessing helps in reducing computational overhead and improving model accuracy.

3. Feature Extraction and Embedding

This layer converts visual data into numerical representations using deep learning models like CNNs (ResNet, Efficient Net) or 3D-CNNs for spatiotemporal feature extraction. These features capture the movements, object shapes, and interactions over time, which are essential for identifying anomalies.

4. Anomaly Detection Engine

The core of the system, this engine uses machine learning or deep learning algorithms to detect out-of-pattern behavior. Models such as Autoencoders, LSTMs, and GANs are commonly used. In unsupervised settings, models learn to

reconstruct normal patterns and flag deviations. In supervised settings, models are trained on labeled datasets of known threats.

5. Alert System and Dashboard

When an anomaly is detected, the system generates alerts via SMS, email, or push notifications. A dashboard visualizes real-time feeds, event logs, threat levels, and allows security personnel to act immediately.

This architecture is often deployed on **hybrid cloud-edge infrastructures**, where time-sensitive processing is handled locally while long-term analysis and retraining are conducted in the cloud.

Anomaly Detection Techniques

Anomaly detection in surveillance is a complex task due to the diverse nature of human behavior and environmental settings. AI models are designed to distinguish between "normal" and "abnormal" activities, even when the anomalies are subtle or context-dependent.

1. Supervised Learning

In this approach, the model is trained on labeled datasets containing both normal and anomalous events. Common algorithms include Support Vector Machines (SVM), Decision Trees, and CNNs. However, supervised learning is limited by the availability of labeled anomalous data, which is rare and expensive to obtain.

2. Unsupervised Learning

This is the most widely used approach for anomaly detection in surveillance. Models learn the normal behavior pattern without needing labeled anomalies. Techniques include:

- **Autoencoders**: Neural networks that reconstruct normal inputs. If reconstruction error is high, the input is likely an anomaly.
- **Principal Component Analysis (PCA)**: Identifies outliers based on variance.
- **Clustering (K-Means, DBSCAN)**: Abnormal events fall outside of dense clusters.

3. Semi-supervised Learning

These models are trained on normal data only. During inference, any deviation from learned patterns is flagged as an anomaly. Variational Autoencoders (VAEs) and LSTM-based sequence models are commonly used here.

4. Deep Generative Models

Generative Adversarial Networks (GANs) are used to generate normal-looking video frames. Discrepancies between real and generated sequences help in identifying anomalies.

5. Temporal Modeling

Many anomalies are temporal in nature (e.g., loitering, sudden running). RNNs, LSTMs, and 3D-CNNs help model time-based dependencies.

The selection of technique depends on the surveillance context (e.g., crowd control vs. perimeter security), availability of data, and deployment infrastructure.

Applications and Case Studies

AI-based surveillance and anomaly detection systems are being actively adopted in various sectors to enhance security, automate monitoring, and improve situational awareness.

1. **Public Safety and Law Enforcement**

Cities like New York and London have integrated AI-powered surveillance systems to monitor public spaces for threats like unattended bags, fights, or abnormal gatherings. These systems reduce response time and help in real-time coordination with law enforcement.

2. **Smart Transportation**

AI surveillance is used in subways, airports, and highways to detect overcrowding, illegal crossings, accidents, or suspicious baggage. For example, the Tokyo subway system uses smart cameras to detect passengers who fall on tracks.

3. **Retail and Commercial Spaces**

Stores use smart surveillance to monitor theft, vandalism, or unauthorized access after hours. Advanced systems also detect customer sentiment, footfall analytics, and queue length.

4. **Industrial Safety**

In manufacturing and construction zones, AI surveillance identifies whether workers are wearing safety gear or entering restricted zones, thereby reducing workplace hazards.

5. **Military and Border Security**

Autonomous surveillance drones and cameras powered by AI scan perimeters for unusual activity such as trespassing or unusual vehicle movements. These systems are crucial in high-risk and remote areas.

Figure 2

Challenges and Ethical Considerations

While AI in surveillance offers significant benefits, it also raises technical, ethical, and legal challenges.

1. **Privacy Invasion**

Surveillance inherently involves monitoring individuals, which can conflict with privacy rights. AI enhances this capacity, potentially enabling **mass surveillance** without consent. There must be legal frameworks and transparency on data collection, storage, and usage.

2. **Bias and Fairness**

AI models may inherit biases from training data. If a model is trained on biased datasets, it might disproportionately target certain communities or individuals, leading to discrimination and unfair profiling.

3. **False Positives and Negatives**

Misclassification of normal behavior as anomalies (false positives) can lead to unnecessary panic or actions. Conversely, false negatives may overlook real threats. Balancing precision and recall is a constant challenge.

4. **Data Annotation and Scarcity**

Labeled surveillance datasets are rare due to ethical and logistical reasons. Most real-world anomalies are rare, making it difficult to train robust supervised models. Synthetic data generation and augmentation are being explored to mitigate this.

5. **Legal and Regulatory Compliance**

Countries have varying laws around surveillance. Systems must comply with **GDPR**, **CCPA**, or other regional data protection laws. Misuse can result in severe penalties.

6. **System Security**

Surveillance systems themselves may become targets of cyberattacks. Ensuring model robustness, data encryption, and access control is crucial for maintaining system integrity.

These challenges necessitate collaboration between technologists, legal experts, ethicists, and policymakers to develop secure, fair, and accountable smart surveillance systems.

Conclusion and Future Scope

AI-powered smart surveillance and anomaly detection represent a paradigm shift in how security is implemented across various sectors. By automating the monitoring process, enhancing accuracy, and enabling real-time response, these systems offer clear advantages over traditional surveillance methods.

Despite current challenges, the field is evolving rapidly. Advances in edge AI, federated learning, and explainable AI (XAI) will further improve the efficiency and transparency of these systems. The use of synthetic data, active learning, and transfer learning will help overcome data scarcity issues.

In the future, surveillance systems will not just detect threats but also predict them using predictive modeling. Integration with other smart city technologies like traffic systems and emergency services will create a holistic, intelligent urban safety net.

However, as the technology advances, so must ethical safeguards. Balancing innovation with privacy, security, and fairness will define the long-term success and social acceptance of AI in surveillance.

References

1. Ullah, W., Ullah, A., Hussain, T., Muhammad, K., Heidari, A. A., Del Ser, J., ... & De Albuquerque, V. H. C. (2022). Artificial Intelligence of Things-assisted two-stream neural network for anomaly detection in surveillance Big Video Data. Future Generation Computer Systems, 129, 286-297.
2. Islam, M., Dukyil, A. S., Alyahya, S., & Habib, S. (2023). An IoT enable anomaly detection system for smart city surveillance. Sensors, 23(4), 2358.
3. Kim, H., & Shon, T. (2022). Industrial network-based behavioral anomaly detection in AI-enabled smart manufacturing. The Journal of Supercomputing, 78(11), 13554-13563.
4. Şengönül, E., Samet, R., Abu Al-Haija, Q., Alqahtani, A., Alturki, B., & Alsulami, A. A. (2023). An analysis of artificial intelligence techniques in surveillance video anomaly detection: A comprehensive survey. Applied Sciences, 13(8), 4956.

5. Atzori, A., Barra, S., Carta, S., Fenu, G., & Podda, A. S. (2021, March). HEIMDALL: an AI-based infrastructure for traffic monitoring and anomalies detection. In 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops) (pp. 154-159). IEEE.
6. Sidharth, S. (2023). AI-Driven Anomaly Detection for Advanced Threat Detection.
7. Ardabili, B. R., Pazho, A. D., Noghre, G. A., Neff, C., Bhaskararayuni, S. D., Ravindran, A., ... & Tabkhi, H. (2023). Understanding policy and technical aspects of ai-enabled smart video surveillance to address public safety. Computational Urban Science, 3(1), 21.
8. Ko, K. E., & Sim, K. B. (2018). Deep convolutional framework for abnormal behavior detection in a smart surveillance system. Engineering Applications of Artificial Intelligence, 67, 226-234.
9. Keerthana, T., Kaviya, K., Priya, S. D., & Kumar, A. S. (2021, May). AI enabled smart surveillance system. In Journal of Physics: Conference Series (Vol. 1916, No. 1, p. 012034). IOP Publishing.
10. Jain, S., & Choudhary, N. (2024, May). AI Techniques for Anomaly Detection in Video Surveillance Using Deep Learning Method. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-6). IEEE.
11. Jayant, P., Vincent, E., Moharir, M., & AR, A. K. (2024, August). Smart health monitoring and anomaly detection using internet of things (iot) and artificial intelligence (ai). In 2024 second international conference on intelligent cyber physical systems and internet of things (icoici) (pp. 479-485). IEEE.
12. Fährmann, D., Martín, L., Sánchez, L., & Damer, N. (2024). Anomaly detection in smart environments: a comprehensive survey. IEEE access.
13. Chevrot, A., Vernotte, A., Bernabe, P., Cretin, A., Peureux, F., & Legeard, B. (2020, December). Improved testing of AI-based anomaly detection systems using synthetic surveillance data. In Proceedings (Vol. 59, No. 1, p. 9). MDPI.
14. Pal, A., Ghosh, P., Roy, S., Das, S., & Mukherjee, S. (2025, January). Advancements in Deep Learning for Smart Surveillance: A Survey on Crime and Anomaly Detection. In 2025 8th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech) (pp. 1-5). IEEE.
15. Rasool, M. (2024). AI-Powered DSPM for Cloud Security: Enhancing Anomaly Detection with Machine Learning.
16. Wang, P., Lin, Y., & Zhao, T. (2024). Smart proctoring with automated anomaly detection. Education and Information Technologies, 1-20.