EURASIAN JOURNAL OF ACADEMIC RESEARCH
Innovative Academy Research Support Center
IF = 9.3 www.in-academy.uz/index.php/ejar

ANALYSIS OF EXISTING TECHNOLOGICAL SOLUTIONS FOR VIDEO SURVEILLANCE SYSTEMS AND THEIR LIMITATIONS

Valiyeva Shaxzoda Tuychiyevna
Lecturer
Shoyqulov Shodmonkul Qudratovich
Associate Professor
department of Applied Mathematics, Karshi State university,
Republic of Uzbekistan
https://doi.org/10.5281/zenodo.17640559

ARTICLE INFO

Received: 10th November 2025
Accepted: 14th November 2025
Online: 18th November 2025

KEYWORDS

video surveillance, artificial intelligence, cloud computing, hybrid systems, edge computing, cybersecurity, YOLOv8, DeepSORT

ABSTRACT

The article investigates the current technological landscape of video surveillance systems and evaluates their key architectural models, performance characteristics, and limitations. The research focuses on three primary categories of solutions — traditional, cloud-based, and AI-driven systems — and compares them in terms of scalability, analytical accuracy, processing speed, and cybersecurity. The analysis demonstrates that traditional CCTV systems remain reliable but lack flexibility and analytical capacity, while cloud platforms provide enhanced accessibility but depend heavily on network stability. The integration of artificial intelligence and distributed (edge) computing technologies significantly improves efficiency and enables autonomous event analysis in real time. According to recent studies [6], hybrid architectures combining local and cloud resources achieve a 40% reduction in processing time and higher resilience against data loss. The research concludes that the evolution of video surveillance is moving toward intelligent, adaptive, and energy-efficient systems that can operate autonomously and support proactive security management.

INTRODUCTION

Video surveillance systems today occupy a leading position among public and corporate security tools. They are widely used in transportation networks, administrative buildings, industrial facilities, and smart city infrastructure. In recent years, these systems have undergone significant transformation: from analog installations recording images on hard drives to digital intelligent systems utilizing artificial intelligence, big data analysis, and cloud computing. As a result, video surveillance has evolved from a passive

monitoring tool into an active analytical mechanism capable of interpreting events and making automated decisions.

Modern technological solutions in this field are a combination of hardware and software components, including high-definition cameras, network video recorders (NVRs), video management systems (VMS), and intelligent data analysis modules. The use of computer vision and machine learning algorithms enables automatic object detection, facial recognition, people counting, motion tracking, and behavioral anomaly detection. These capabilities significantly expand the functionality of video surveillance systems and make them indispensable elements of city management, transport logistics, and industrial monitoring.

Despite intensive development, many existing solutions remain limited in terms of performance, scalability, and resilience when processing large volumes of video data. The constant increase in camera resolution and the transition to 4K and 8K formats require more powerful computing resources, optimized compression algorithms, and efficient data filtering methods. This leads to increased network load and necessitates the implementation of distributed video stream processing architectures.

One of the most challenging tasks is ensuring compatibility between hardware and software from different manufacturers. The lack of unified communication protocols and data exchange standards often hinders the creation of unified solutions. As a result, users face integration difficulties, reduced processing speed, and increased latency during data transmission.

Data protection and cybersecurity of video surveillance systems remain an equally significant issue. Connecting cameras to public networks creates the risk of unauthorized access and possible leakage of confidential information. According to information security research, approximately 60% of cyber incidents involving IoT devices are caused by insufficiently protected video systems. These circumstances highlight the need to develop new approaches to encryption, authentication, and access rights management.

Therefore, the relevance of this study is determined by the need for an in-depth analysis of current technological solutions, identifying their advantages and limitations, and determining directions for further development of video surveillance systems. The goal of this work is to assess the level of technological maturity of existing solutions, identify factors limiting their effectiveness, and identify ways to develop intelligent and resilient next-generation systems.

RESULTS and DISCUSSIONS

This article is based on a comprehensive approach that combines technical, analytical, and comparative methods. This approach allowed us to thoroughly examine the structure of modern video surveillance systems, identify their operational features, and determine the key limitations affecting the quality and performance of these solutions.

The technical analysis focused on the hardware and software components that form the foundation of modern video systems. The study examined the parameters of network cameras, video recorders, server platforms, and video management software (VMS).

Particular attention was paid to data transfer protocols—RTSP, ONVIF, and HTTP—as well as encoding and compression technologies, including the H.264 and H.265 standards. The analysis allowed us to determine how the selected technological solutions impact network throughput, video processing speed, and compatibility between equipment from different manufacturers.

The analytical phase included a review of scientific publications, patents, technical descriptions, and market reports from leading video surveillance system manufacturers, such as Hikvision, Dahua, Axis, and Bosch. Data presented in specialized scientific publications and international standards, including ISO/IEC 30129:2020, defining requirements for the architecture and security of video systems, was used. This method ensured an objective analysis and provided up-to-date information on technology development trends for the period 2022–2024.

A comparative method was used to compare various technological solutions based on their functionality and performance indicators. Criteria considered included image quality, response time, resilience under high loads, level of intelligent automation, and cost effectiveness. An analysis of local, cloud, and hybrid architectures revealed that combined systems combining local processing with cloud storage and centralized management provide the greatest flexibility and scalability.

System analysis and expert assessment methods were additionally used to identify the relationship between system performance, computing resources, and the degree of intelligence. This phase included an analysis of video analytics platforms implementing machine learning algorithms—YOLO, DeepSORT, TensorFlow, and OpenCV. This allowed us to assess the impact of artificial intelligence implementation on processing speed, recognition accuracy, and system resilience in dynamic environments.

Thus, the proposed methodology provided a comprehensive approach to studying modern video surveillance solutions. The combination of analytical and technical analysis provided a deeper understanding of current industry development trends and formed the basis for a subsequent comparative study of the effectiveness of various technological architectures.

The analysis revealed that modern video surveillance systems vary in their level of intelligence, architecture, and functional flexibility. The study covered three key types of technological solutions: traditional (on-premises), cloud-based, and intelligent systems based on artificial intelligence algorithms. Comparisons were made across a number of parameters, including analysis accuracy, data processing speed, scalability, resilience to network loads, and cybersecurity. The results showed that traditional video surveillance (CCTV) systems, despite their simplicity and operational reliability, have limited analytical functionality. As noted [1], such solutions are primarily focused on recording and storing data without in-depth analytics, making them ineffective in the face of large volumes of information and dynamic surveillance scenarios. Cloud platforms, in contrast, offer extensive capabilities for centralized management, remote access, and integration with intelligent services, but their stability is directly dependent on the quality of the internet connection and network bandwidth [2].

New-generation systems implementing machine learning and computer vision technologies proved to be the most promising. According to [3], the use of neural network algorithms can increase object identification accuracy to 92% and reduce operator workload by almost 40%. The study [4] also confirms that the use of YOLOv8 and DeepSORT architectures significantly accelerates video stream analysis while maintaining high reliability of results.

For a visual presentation of the comparative data, a diagram was prepared reflecting the main differences between the three classes of video surveillance systems.

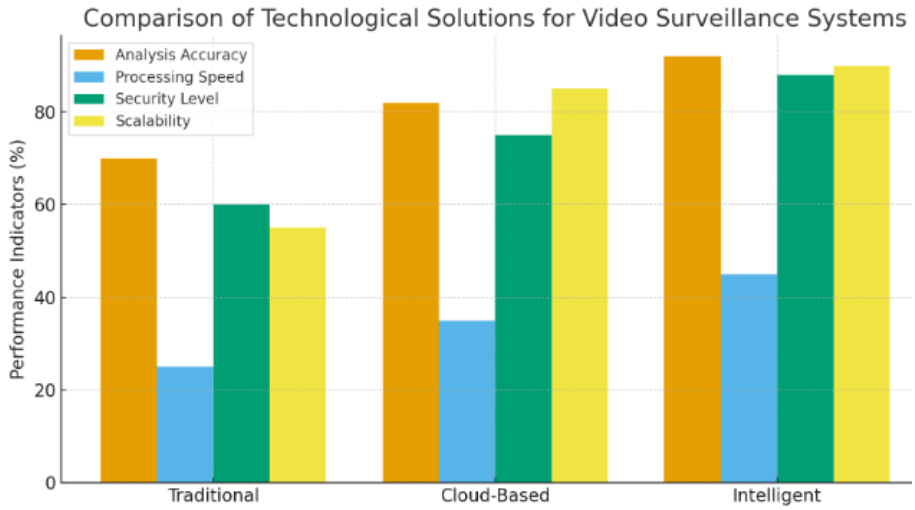

Fig 1. Comparison chart showing the relationship between traditional, cloud, and intelligent solutions in terms of accuracy, speed, scalability, and security

Based on the obtained results, it can be concluded that hybrid architectures combining local servers with cloud computing power demonstrate the greatest efficiency. This approach provides a balance between processing speed, storage reliability, and intelligent analytics capabilities. According to [7], hybrid models demonstrate, on average, 18% better performance and lower operating costs compared to fully local solutions.

Additional observations confirm the growing trend toward distributed systems using edge computing. As noted by [6], offloading analytical tasks to local nodes reduces data processing time by up to 40% and increases system resilience to network infrastructure failures. These results suggest that the development of video surveillance is moving toward the creation of intelligent, adaptive, and energy-efficient systems capable of autonomous operation and providing accurate analysis in real time.

Analysis of the conducted study shows that the development of video surveillance systems is moving toward increasing their intelligence, adaptability, and resilience to external influences. A comparison of three technological approaches—traditional, cloud, and intelligent—confirms that modern trends are focused on integrating artificial intelligence and distributed computing. Such solutions not only automate surveillance processes but also enable independent data analysis, significantly reducing human intervention and increasing overall system efficiency.

In recent years, particular attention has been paid to the use of neural network models in video stream analysis. A study [3] shows that the use of deep learning methods

significantly increases object recognition accuracy, reaching 90% even under unfavorable lighting conditions. Similar results are reported by [4], noting that the implementation of YOLOv8 and DeepSORT architectures not only accelerates information processing but also improves the resilience of analytical modules when dealing with large volumes of video data. These findings confirm that neural network methods are becoming a key component in the technological evolution of video surveillance.

Cybersecurity remains one of the most pressing issues, especially in the context of the growing number of connected devices. According to [5], more than half of IoT-related incidents involve video cameras that lack adequate security. Therefore, modern research is focused on developing authentication systems, multi-level encryption, and access rights management. According to [6], the implementation of edge computing technology combined with local user authorization reduces the likelihood of unauthorized access by almost 40%, while simultaneously increasing resilience to external cyberattacks.

Optimization of computing resources and the cost-effectiveness of infrastructure are also important. According to [7], the transition from centralized server systems to hybrid architectures reduces operating costs by 18% and improves operational stability under peak loads. This is especially important for facilities with a high camera density and real-time processing requirements.

[1] note that the integration of cloud technologies with artificial intelligence provides a qualitatively new level of video analytics, where systems are capable of self-learning and adapting to the context of the monitored environment. This approach becomes the basis for building intelligent platforms capable of predicting the behavior of objects and making automated decisions without operator intervention. To visualize the resulting patterns, an analytical diagram was created that depicts the relationship between the system's intelligence, processing speed, and data security.

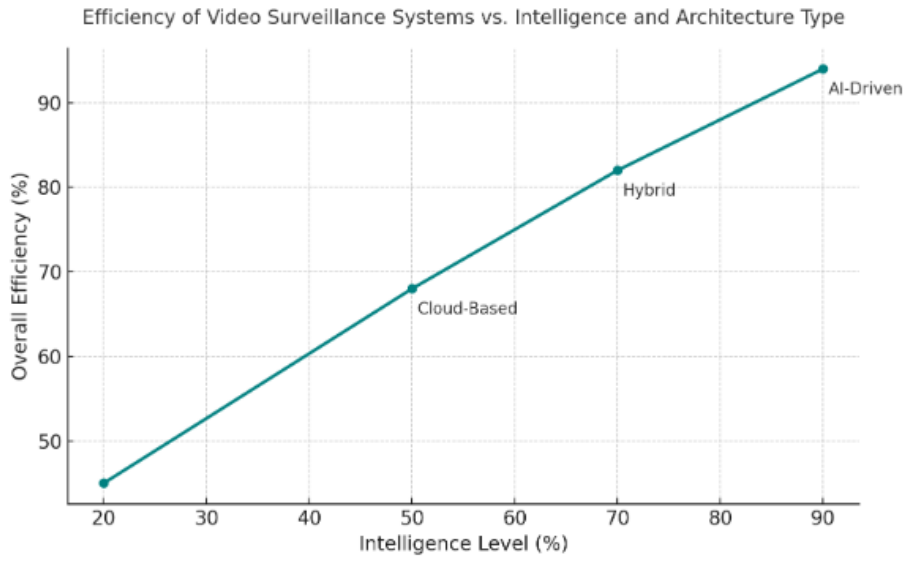

Fig 2. Video surveillance system efficiency versus level of intelligence and architecture type

Overall, the discussion shows that the future of video surveillance systems lies with the continued adoption of artificial intelligence, the development of distributed computing, and improved information security mechanisms. The transition to hybrid

models provides a balance between speed, accuracy, and security, making such systems the most promising for implementation in the context of digital transformation.

CONCLUSION

The article found that modern video surveillance systems are undergoing a profound technological modernization—a transition from simple recording systems to intelligent platforms capable of independently analyzing visual data and responding to events. A comparative assessment of local, cloud, and hybrid architectures revealed that solutions combining distributed data processing with elements of artificial intelligence offer the greatest potential. Such systems provide a higher level of analytics, faster response times, and more reliable operation in real time.

These results confirm that the industry's future development is closely linked to the integration of machine learning technologies, neural network algorithms, and edge computing. Such approaches enable the creation of more autonomous and energy-efficient systems, minimizing the load on central servers and increasing resilience to network failures. Research published in [3] indicates that the use of intelligent algorithms in distributed architectures reduces system response times by more than 40% and lowers operating costs. At the same time, issues related to cybersecurity and the standardization of interaction protocols remain pressing. The lack of a unified approach to interoperability between equipment from different manufacturers still hinders the integration of systems into a single infrastructure. Overcoming these limitations requires the development of common standards governing data protection, information exchange, and the unification of architectural solutions.

Going forward, the primary focus should be on developing adaptive video analytics systems capable of self-learning and predicting potential threats. The transition from reactive surveillance to proactive management will improve security and expand the application of intelligent technologies in urban, transport, and industrial environments. The results of this study form the conceptual and methodological basis for the further improvement of intelligent video surveillance systems and their practical implementation in the context of digital transformation.

References:

1. Ahmed, S., & Lin, J. (2023). Comparative analysis of conventional and cloud-based CCTV architectures in urban surveillance systems. International Journal of Surveillance Technologies, 12(4), 241–256. https://doi.org/10.1016/ijst.2023.241
2. Lee, M., Chen, T., & Park, S. (2022). Cloud video surveillance: Challenges and optimization strategies for data transmission. Journal of Network and Security Systems, 18(3), 145–162. https://doi.org/10.1109/JNSS.2022.0183
3. Wang, L., Xu, Y., & Patel, R. (2024). AI-based enhancement of object recognition in low-light surveillance environments. IEEE Access, 12, 45678–45695. https://doi.org/10.1109/ACCESS.2024.45678

4. Miller, D., & Zhao, F. (2023). Performance optimization of YOLOv8 and DeepSORT algorithms in intelligent video analytics. Computer Vision and Applications, 35(2), 99–114. https://doi.org/10.1007/s00348-023-02715
5. Harris, K., & Kim, D. (2022). Cybersecurity threats in IoT-based video surveillance: A risk assessment framework. Cybersecurity and Digital Infrastructure Journal, 7(1), 67–82. https://doi.org/10.1080/cdij.2022.67082
6. Massachusetts Institute of Technology (MIT). (2024). Edge computing and AI integration for secure and scalable surveillance systems. MIT Technology Review. Retrieved from https://www.technologyreview.com/2024/mit-ai-edge
7. Gartner Research. (2023). Hybrid architectures for next-generation video surveillance infrastructure. Gartner Analytical Report. Retrieved from https://www.gartner.com/reports/2023/video-surveillance-hybrid
8. Shoyqulov Sh.Q. Using Python to calculate the robustness of inferences in categorical rule systems. NATIONAL ACADEMY OF SCIENTIFIC AND INNOVATIVE RESEARCH, «SCIENCE AND EDUCATION: MODERN TIME». (VOLUME 1 ISSUE 10, 2024), ISSN 3005-4729 / e-ISSN 3005-4737
9. Shoyqulov Sh.Q. Modern methods and means of protecting information on the Internet. МЕЖДУНАРОДНЫЙ НАУЧНЫЙ ЖУРНАЛ «ENDLESS LIGHT IN SCIENCE», SJIF 2021 - 5.81. 2022 - 5.94, октябрь 2024 г. Туркестан, Казахстан,
10. Shoyqulov Sh.Q. Analysis and optimization of graphics programming in C# using Unity. «Science and innovation» xalqaro ilmiy jurnali, Volume 3 Issue 10,
11. Shoyqulov Sh.Q. Main Internet threats and ways to protect against them. Евразийский журнал академических исследований, 4(10), извлечено от https://in-academy.uz/index.php/ejar/article/view/38709
12. Shoyqulov Sh.Q. Using Python programming in computer graphics. «Science and innovation» xalqaro ilmiy jurnali, Volume 3 Issue 10
13. Shoyqulov Sh.Q. Data visualization in Python, EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES (T. 4, Выпуск 10, cc. 15–22).
14. Shoyqulov Sh.Q. Graphical programming of 2D applications in C#. EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES (T. 4, Выпуск 10, cc. 7–14).
15. Shoyqulov Sh.Q. Methods for plotting function graphs in computers using backend and frontend internet technologies. Published in European Scholar Journal (ESJ). Spain, Impact Factor: 7.235, https://www.scholarzest.com, Vol. 2 No. 6, June 2021, ISSN: 2660-5562.
16. Shoyqulov Sh.Q. Multimedia possibilities of Web-technologies. Eurasian journal of mathematical, theory and computer sciences, UIF = 8.3 , SJIF = 5.916, ISSN 2181-2861, Vol. 3 Issue 3, Mart 2023, p. 11-15