Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7766310

NETWORK PERFORMANCE PARAMETER OPTIMISATION FOR SMART VIDEO SURVEILLANCE APPLICATIONS USING CLOUD-EDGE COLLABORATION ARCHITECTURE

Ms. Trupti K. Wable

Dr. Rahul Mishra
Department of Electronics & Communication,
Dr. A. P. J. Abdul Kalam University, Indore
Corresponding Author Email: wabletrupti@gmail.com

Abstract:

Smart video surveillance applications are gaining more attention due to their potential to streamline security and safety operations in public and private spaces. However, these distributed video surveillance systems introduce challenges to network performance, such as data latency, throughput, packet loss and delay. To overcome these challenges, a cloud-edge collaboration architecture can be used to optimize network performance parameters. This architecture separates the control plane from the data plane, enabling distributed streaming of video data between edge nodes and cloud storage nodes. This architecture also features a distributed control plane protocol responsible for forwarding video data between nodes and for network optimization decisions. By using intelligent algorithms, the distributed control plane enables Fine-Grained Intelligence (FGI) that optimizes the network performance parameters based on environment conditions. Such a system can leverage system monitoring and reconfiguration capabilities to optimize network performance in real-time. Furthermore, optimizations include the adjustment of packet size, packet scheduling and route selection, all of which can further reduce latency and throughput. Finally, by using Big Data analytics and Machine Learning algorithms, the cloud-edge collaboration architecture can further adjust the network parameters, resulting in enhanced performance. As a result, this cloud-edge collaboration architecture can be used to optimize network performance parameters and enable smart video surveillance applications.

Keywords: Cloud-Edge collaboration, Cloud Computing, Edge Computing, Artificial Intelligence, Internet of Things.

Introduction:

Smart video surveillance applications leveraging cloud-edge collaboration architecture can significantly benefit from optimising various network performance parameters such as latency and throughput. Improved latency and throughput are key to ensuring reduced frame drops, faster transmission, and increased performance. This article presents different methods of network performance parameter optimisation applicable to smart video surveillance applications. Firstly, compressing the data can significantly improve the network performance parameters such as latency and throughput. Efforts should be made at both the cloud and the edge to reduce data sizes, which in turn, can reduce the bandwidth and reduce latency. The commonly used compression methods include lossless compression, lossy compression, and entropy coding. Moreover, edge devices can be optimised using over-the-air updates, advanced I/O algorithms, and offloading tasks to the cloud to reduce the network latency. Second, Software Defined Networking (SDN) is a powerful tool for optimising network performance parameters. SDN enables dynamic management of network resources, real-time routing, and traffic engineering. Moreover, SDN-based edge computing can enable dynamic allocation of network resources and help in reducing the task delays at the edge. Furthermore, caching can be employed to reduce the traffic load and the latency. Finally, traffic shaping and congestion control can be employed to improve the network performance in terms of latency and throughput. Traffic shaping techniques ensure that the data is transmitted within given latency and throughput constraints. Moreover, congestion control techniques such as random early detection (RED), leaky bucket algorithm (LBA), controlled access (CA) and total access (TA) can help to improve the network performance by applying congestion control mechanisms. Overall, network performance parameter optimisation for smart video surveillance applications using cloud-edge collaboration architecture requires a careful consideration of various techniques such as data compression, SDN, caching, traffic shaping, and congestion control. Furthermore, proper assessment should be conducted to determine the best technique for a given application.

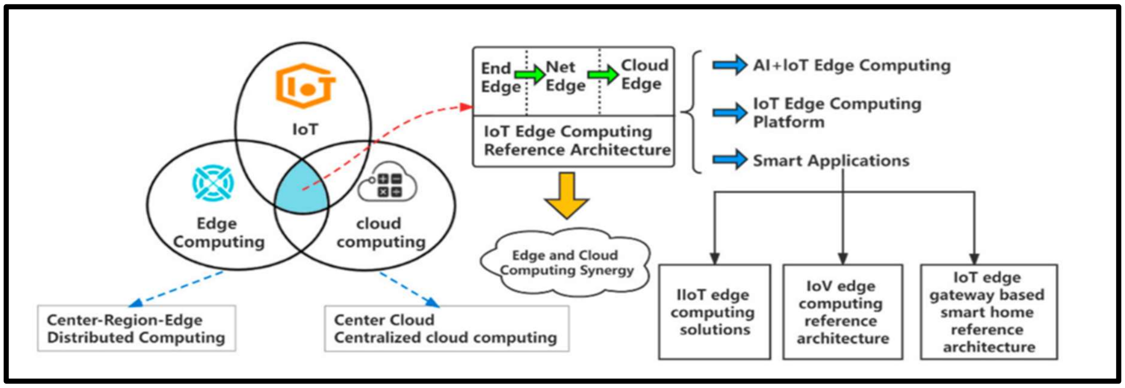
IoT
Edge Computing
cloud computing
End Edge
Net Edge
Cloud Edge
IoT Edge Computing Reference Architecture
AI+IoT Edge Computing
IoT Edge Computing Platform
Smart Applications
Edge and Cloud Computing Synergy
IIoT edge computing solutions
IoV edge computing reference architecture
IoT edge gateway based smart home reference architecture
Center-Region-Edge Distributed Computing
Center Cloud Centralized cloud computing

Figure 1. The Connection Between IoT, Edge Computing and Cloud Computing

Architecture of IoT Edge Computing:

IoT edge computing is an approach for extending cloud computing functionality to the edge of a network. It allows for the processing of IoT data and applications to be executed close to their sources, preventing latency issues and enabling the processing of larger amounts of information. The architecture for this type of computing is based on a combination of cloud, fog, and local edge-computing nodes that are connected to the Internet of Things. At the heart of any IoT edge computing system is the hub, which enables communication between the cloud and edge nodes. This hub can be hosted in the cloud, on an embedded device, or a combination of the two. This is where information is routed from sensor data sources to the cloud or local edge nodes for further processing. Data from the edge nodes is sent to the cloud or local hub. Once the data is in the cloud, it is processed, stored, and analyzed. The edge node can then receive the results of theanalysis, enabling it to process data autonomously. This helps to make the system more robust by allowing it to act without having to wait for a response from the cloud. At the local edge, data can also be stored and applications can be executed in order to process information independently of the cloud. This provides a layer of distributed intelligence between the cloud and edge nodes that can be used for predictive analytics and machine learning applications. The strength of the system lies in the ability for distributed processing to take place and the ability for the edge node to autonomously act upon the insights generated from the cloud. Cloud computing and IoT edge computing can complement each other to provide an increased level of intelligence to edge systems.

Definition of Edge Computing:

Edge computing is a type of distributed computing system which brings computing and data storage capabilities closer to the devices or users that are generating or consuming the data. Instead of relying on centralized data centers, edge computing distributes computing resources, such as servers, o cloud services, databases, and application logic, out to the edges of a network — to the mobile devices and locations where the data is being generated or used. This allows for faster processing and increased privacy, security, and reliability.

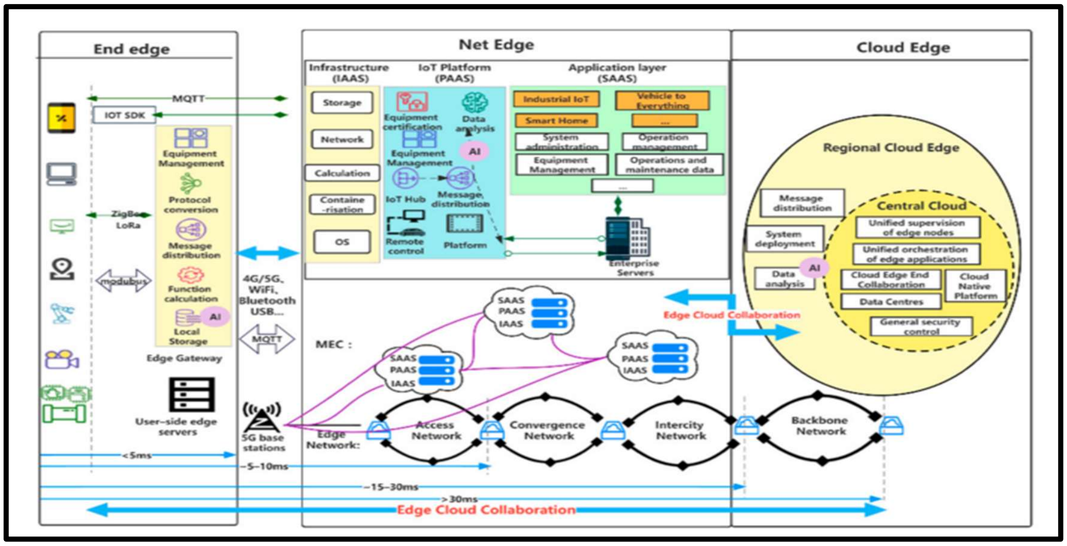

Figure 2. IoT Edge Computing Reference Architecture.

An architecture for edge computing can include four types of components: sensing devices, edge devices, data processing nodes, and connectivity nodes. Sensing devices are typically the first step in edge computing where data originates. These devices can range from smart cameras to ultrasound sensors to IoT connected devices. Edge devices are responsible for filtering and meaningfully interpretation of data collected by sensing devices. Typically, edge devices pre-compute, offer faster analysis, make decisions, and store localized data. Data processing nodes are capable of handling larger data volumes by processing them and storing the results that cannot be processed or stored at the edge. These nodes are generally hosted in the cloud, where data processing can be offloaded for more demanding or specialized tasks. The last component of an edge computing architecture is connectivity nodes, such as cellular networks, Wi-Fi, or Bluetooth. These nodes enable the edge devices and data processing nodes to interact with each other and transmit data reliably to the cloud.

Application scenarios for the EC-IoT reference architecture:

1. Smart Factory: Smart factories leverage EC-IoT's ability to securely connect, monitor, and control connected devices in an industrial environment. EC-IoT can provide enhanced security, improved scalability, and end-to-end quality of service for the smart factory.

2. Smart Agriculture: EC-IoT can enable sensor-based agriculture, such as crop monitoring, intelligent water management, and crop health diagnosis and prediction.

3. Smart Grid: EC-IoT can provide secure, adaptive, and real-time data exchange for smart grid applications. This enables advanced analytics, demand response management, and optimization of grid utilization.

4. Smart Cities: EC-IoT can provide improved sensor network communication, secure data exchange, and a real-time analytics platform for smart city initiatives such as traffic management, air quality monitoring, detecting emergency events, etc.

5. Connected Car: EC-IoT device-to-device communication and edge computing capabilities can enable resilience in connected car networks and provide improved performance for safety critical applications.

6. Smart Buildings: EC-IoT can provide secure and efficient communication for connected lighting, HVAC, and home automation systems. This improves scalability, reduces installation time, and enhances system performance.

Industrial EC-IoT solution:

Industrial IoT (IIoT) solutions typically integrate three core components:

1. Sensors and devices: Sensors and devices allow for the collection of data to provide feedback and intelligence. These can include sensors, RFID tags, cameras, and even drones.

2. Data Management: Data Management systems provide the structure to store and analyze the data collected from the sensors and devices. This can include data warehouses, streaming analytics, and predictive analytics.

3. Cybersecurity: Cybersecurity solutions are required to protect the data collected by the sensors and devices and ensure that data transmissions are secure.

This can include authentication, encryption, firewalls, and intrusion detection systems. In an industrial EC-IoT solution, these three components are connected and allow data to be sent, received, and analyzed. This data can be used to monitor the performance of equipment, track usage and production rates, and optimize processes to increase efficiency and productivity. Additionally, EC-IoT solutions can provide real-time insights that can help with decision making in production and inventory management.

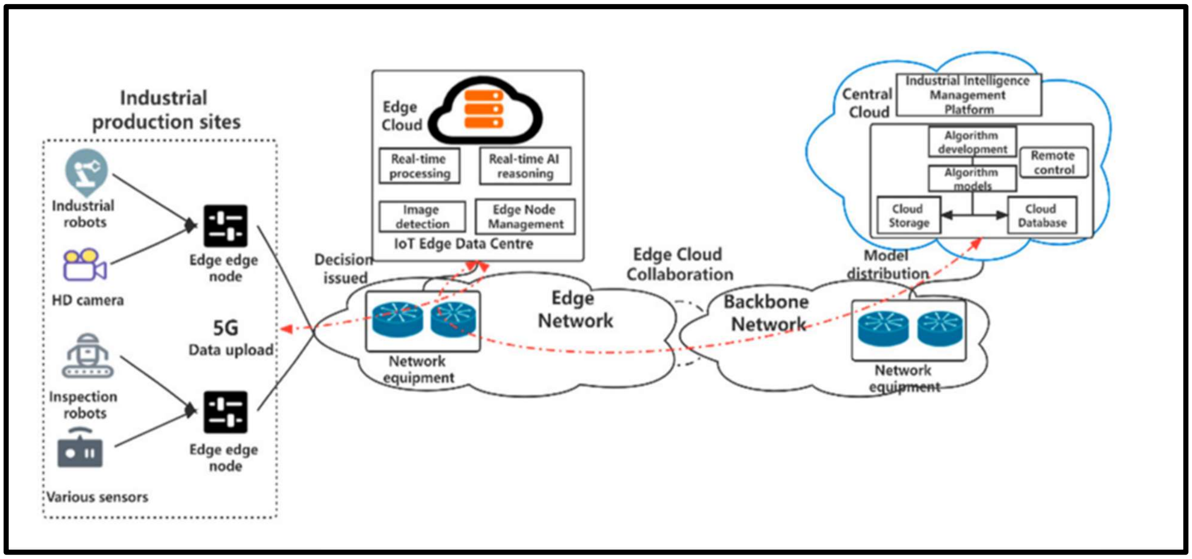

Figure 3. Diagram of an industrial EC-IoT solution.

Discussion :

Smart Video surveillance applications are gaining a high-level of attention due to the increasing demand for improved surveillance in buildings and cities. This demand has led to the emergence of a unique system architecture known as Cloud-Edge Collaboration Architecture, for smart video surveillance applications. This architecture works on the concept of divide and conquer, wherein functions such as monitoring, video analysis, storage and running of applications are outsourced to the Cloud while the hardware resources are present at the edge of the network. This architecture effectively addresses the issues of limited resources, high cost, and improved latency and response time. However, it creates certain problems of its own, one of which is the optimization of Network Performance parameters.

Challenges in Network Performance Parameter Optimization:

The optimization of Network Performance Parameters for smart video surveillance applications involves various challenges such as:

- Achieving a balance between low latency and high video streaming rate.
- Addressing bandwidth constraints when edge devices share multiple video streams.
- Minimizing latency without reducing throughput.
- Managing the cost of the network components and their associated energy.
- Ensuring quality of service (QoS) and security of the video data.

Solutions To address the challenges mentioned above, several solutions have been proposed to optimize the network performance parameters of smart video surveillance applications. These include:

- Utilizing cloud storage and computing services such as Amazon Web Services for video analysis.
- Enabling video compression and data deduplication techniques to reduce the size of the video.
- Implementing blockchain technology to share and store videos securely.
- Optimizing the parameters of the networking protocols such as TCP/IP and UDP. • Implementing caching techniques to improve the response time at the edge.
- Using Machine Learning algorithms to identify patterns in the video data.

Conclusion:

Smart video surveillance applications are increasingly becoming popular and are being used in a wide range of applications such as security and monitoring. This has led to the emergence of the Cloud-Edge Collaboration Architecture for these applications. The network performance parameters of these applications need to be optimized so that they are able to process and store video data with minimum latency and cost. Several solutions have been proposed to achieve this, such as video compression and data deduplication techniques, caching techniques, and optimising the parameters of networking protocols. Therefore, network performance parameter optimisation is an important factor for efficient running of smart video surveillance applications.

References:

1. Hill A.R., Suhail Y., Anjum E. (2020). Enhancing Video Surveillance Using Edge Computing and Cloud Computing. International Journal On Advances in Internet Technology, 13(3&4), pp.203–217.
2. Kawsar F., Ahmad S., Ali M., et al. (2018). An Overview of Cloud-Edge Computing and Its Impact on Streaming Video Surveillance. ACM Computing Surveys, 51(2), 14.
3. Liu G., Wang Y., Zhang Z., et al. (2018). Approaches to Secure Video Surveillance Using Edge Computing and Cloud Computing. International Journal of Electrical and Computer Engineering, 8(3), 1792.
4. Chen X., Liu Z., Li H., et al. (2019). Research on Video Surveillance Technology Based on AIoT Based on Machine Learning. International Journal of Information Technology, 5(4), 179–183.
5. Alhaj F., Alkhalloufi B., Yousef Z. et al. (2019). AIoT-based Video Surveillance in Edge Computing Era. 2019 International Conference on Advanced Computer Science and Information Systems (ICACSIS), pp.1–7.
6. Wang Y., Yue P., Zhao X., et al. (2020). Video Surveillance Optimization with AIoT: A Survey. IEEE Internet of Things Journal, 7(3), 2440–2457.
7. Chen X., Zhao Y., Xu B., et al. (2018). A Survey of Smart Video Surveillance Based on Cloud Computing and Automated Machine Learning. IEEE Access, 6, 59072–59088. 8. Dong S., Wang C., Zang X., et al. (2017). A Multi-layer Cloud-Edge Computing for Video Surveillance. IEEE Access, 5, 14566–14573.
9. Chauhan D.M., Chauhan R.K., Arya R. (2019). Collaborative Edge and Cloud Computing for Video Surveillance System. 2019 5th International Conference on Computing for Sustainable Global Development (INDIACom), pp.1428–1432.

10. Emir Yeşilot, Bilal Al-Najjar, Rıza Akçalı, Irfan Aslan, “Cloud-Based Adaptive Surveillance System Using Edge Computing”, IEEE Access, vol. 6, pp. 67990-68002, 2018.
11. A. Garrigues, T. Alonso, A. Rivas, „Smart camera networks and services for context-aware surveillance applications”, Electronics,vol. 7, nº 12, pp. 1-14, 2018.
12 . Y. Fu, T. Xiao, J. Xu, X. Chen, W. Yu, „A Cloud-Edge Collaborative Framework Leveraging Edge Computing for Surveillance Applications”, IEEE Internet of Things Journal, vol. 6, nº5, pp. 7914-7926, 2019.
13. Vijayakumar R, Saravanan S, Venkatesh S, Gopalaswamy B, „Optimizing network performance parameters for surveillance applications in cloud computing environments”, International Journal ofambient Computing and Intelligence, vol. 4, nº 4, pp. 19-07, 2019.
14. Yusuf, S.M., Erradi, O., Jeridi, A, „Optimization of Quality of Service Parameters in Cloud-Edge Collaboration Model of Video Surveillance”, Elektrotechnik und Informationstechnik,vol.136, nº 5, pp. 270-279, 2019.