International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT)

Koffka Khan[1]
[1]Department of Computing and Information Technology, Faculty of Science and Agriculture, The University of the West Indies, St. Augustine Campus, TRINIDAD AND TOBAGO.
Email address: koffka.khan@gmail.com

Abstract— *The Video Streaming in Industrial IoT (VSIIoT) Taxonomy provides a comprehensive framework for categorizing and understanding the multifaceted aspects of video streaming within the context of the Industrial Internet of Things (IIoT). This taxonomy encompasses various dimensions, including network architecture, streaming protocols, video quality, latency, camera types, security measures, use cases, integration with other IIoT technologies, data storage, analytics, scalability, regulatory compliance, user access, and budget considerations. By utilizing the VSIIoT Taxonomy, organizations and professionals can effectively design, implement, and manage video streaming solutions tailored to their specific IIoT applications and requirements.*

Keywords— *Video: Streaming: IIoT: Taxonomy.*

I. Introduction

The integration of video streaming technology [6], [5], [10] within the Industrial Internet of Things (IIoT) ecosystem [20], [4], [3] has ushered in a new era of data-driven decision-making and operational efficiency. Video feeds from cameras and other visual sensors are providing critical insights into industrial processes, enabling real-time monitoring, predictive maintenance, and enhanced security. To navigate the complex landscape of video streaming in IIoT, a structured framework is indispensable. This introduction serves as a gateway to understanding the Video Streaming in Industrial IoT (VSIIoT) Taxonomy, a comprehensive and adaptable system for categorizing and organizing the diverse elements of video streaming in an industrial context.

The Era of Visual Data in IIoT:

The Industrial Internet of Things (IIoT) has transformed the way industries operate and manage their assets. The ability to connect, monitor, and control a myriad of devices and sensors has resulted in increased productivity and cost savings. In this landscape, the role of video streaming is pivotal. Real-time and archived video feeds offer insights into every facet of industrial operations, be it surveillance, predictive maintenance, quality control, or process optimization. Video data augments traditional sensor data with a rich visual layer, enabling a more comprehensive understanding of the industrial environment.

The Need for Structured Classification:

As the importance of video streaming in IIoT grows, so does the complexity of its implementation. Various aspects come into play, from the choice of network architecture and streaming protocols to camera types and data storage options. Furthermore, the security and regulatory requirements in industrial settings demand careful consideration. In response to this intricate landscape, the VSIIoT Taxonomy has been developed to provide a structured and coherent framework for understanding and implementing video streaming solutions in the context of IIoT. By categorizing these diverse elements, organizations and professionals can make informed decisions, tailor their solutions to specific needs, and ensure the seamless integration of video streaming into their industrial processes. This taxonomy's adaptability and depth make it an indispensable tool in harnessing the power of video streaming within the Industrial Internet of Things.

In Section II we outline the motivation driving the AVQOES taxonomy. In Section III we give the taxonomy components while a comparison among the components is given in Section IV. In Section V the uses of the AVQOES is given. In Section VI a discussion of the taxonomy is given. Finally, the conclusion is given Section VII.

II. Motivation for the Taxonomy

The motivation for creating the Video Streaming [7], [8], [9] in Industrial IoT (VSIIoT) Taxonomy is driven by several key factors and needs within the industrial landscape:

Rapid Growth of IIoT: The Industrial Internet of Things (IIoT) has witnessed substantial growth in recent years, with industries increasingly leveraging data and connectivity for improved efficiency, safety, and competitiveness. Video streaming plays a pivotal role in this transformation.

Diverse Applications: Video streaming is used in a wide range of industrial applications, from surveillance and security to process optimization, predictive maintenance, and quality control. Each application has unique requirements and considerations.

Complex Ecosystem: The IIoT ecosystem is complex, involving various devices, networks, and technologies. A comprehensive taxonomy helps stakeholders understand the components and relationships involved in video streaming.

Regulatory and Security Challenges: Industries, especially those related to critical infrastructure and sensitive data, face stringent regulations and security concerns. Proper classification and understanding of video streaming practices are vital for compliance and risk management.

Technological Advancements: The field of video streaming is continually evolving with new technologies, protocols, and approaches. A taxonomy helps capture these advancements and their implications on industrial applications.

Decision-Making: Organizations need to make informed decisions when selecting video streaming solutions. A well-structured taxonomy provides a clear framework for evaluating options and aligning them with specific needs and objectives.

Operational Efficiency: Optimizing industrial operations is a key goal of IIoT. Understanding the taxonomy allows organizations to make choices that improve operational efficiency, reduce costs, and enhance performance.

Data-Driven Insights: Video data is a valuable source of insights and intelligence in industrial settings. Proper classification ensures that data is leveraged effectively to support data-driven decision-making.

Scalability and Flexibility: Many industrial operations are subject to growth and change. A taxonomy accounts for the scalability and adaptability of video streaming solutions to accommodate evolving needs.

Risk Mitigation: In industries where security and safety are paramount, understanding the taxonomy helps in the selection of solutions that minimize risks and vulnerabilities.

In summary, the motivation for the VSIIoT Taxonomy lies in its ability to provide clarity, structure, and guidance in the complex and dynamic field of video streaming in the industrial context. By categorizing and defining various aspects of video streaming, the taxonomy aids organizations and professionals in making informed decisions, complying with regulations, and optimizing their use of video data within the IIoT landscape.

III. VSIIoT Taxonomy

The Video Streaming in Industrial IoT (VSIIoT) Taxonomy is a comprehensive framework designed to bring order and clarity to the intricate world of video streaming within the context of the Industrial Internet of Things (IIoT). In a landscape where the convergence of visual data and industrial processes is becoming increasingly critical, this taxonomy serves as an essential guide for understanding, classifying, and optimizing the various dimensions of video streaming in IIoT.

Navigating the Complexities:

The realm of IIoT is marked by its diversity, encompassing applications such as surveillance, predictive maintenance, quality control, and process optimization. Video streaming has emerged as a versatile tool for enhancing these industrial processes, but its successful implementation is a multidimensional task. Choices need to be made regarding network architecture, streaming protocols, video quality, latency, camera types, security measures, and more. The VSIIoT Taxonomy provides a structured and logical framework that enables organizations and professionals to navigate these complexities.

A Unified System for Classification:

The VSIIoT Taxonomy classifies the myriad aspects of video streaming in IIoT under distinct categories, allowing for a systematic breakdown of considerations. Whether you are dealing with securing sensitive video data, optimizing network infrastructure, or integrating visual data with sensor readings, this taxonomy offers a structured approach to guide decision-making and implementation. By adopting this unified system, organizations can better understand their requirements and tailor video streaming solutions to meet their specific goals, ensuring that their IIoT projects are not only efficient but also future-proof. In the ever-evolving landscape of IIoT, the VSIIoT Taxonomy provides a roadmap for harnessing the full potential of video streaming technologies.

Video streaming in Industrial Internet of Things (IIoT) can be categorized into various dimensions, considering different aspects of the technology and application. Here's a taxonomy of video streaming in IIoT:

A. Network Architecture [15], [17], [13]:

Edge Streaming: Video data is processed and streamed at the edge of the network, closer to the data source.

Cloud Streaming: Video data is sent to a central cloud server for processing and storage before being streamed to end-users or devices.

Here are further details:

In the context of the Video Streaming in Industrial IoT (VSIIoT) Taxonomy, the classification of network architecture plays a fundamental role in determining how video data is processed and distributed. This taxonomy acknowledges the two primary approaches to network architecture used in the realm of video streaming in IIoT: Edge Streaming and Cloud Streaming.

1. Edge Streaming:

Edge Streaming represents a network architecture that emphasizes processing and streaming video data at the edge of the network, closer to the data source, which is typically where the cameras or sensors capturing the video are located. This approach minimizes the data's round-trip journey to remote data centers or cloud servers. Here are some key aspects of Edge Streaming:

Low Latency: Edge streaming is known for its low-latency characteristics. By processing and streaming video data locally, it significantly reduces the time it takes for the data to reach end-users or devices. This is essential for applications where real-time monitoring and quick decision-making are critical, such as surveillance and safety systems.

Bandwidth Efficiency: Edge streaming can be more bandwidth-efficient than cloud streaming, as it only transmits data when necessary. Video data is processed locally, and only relevant information or detected events trigger data transmission. This reduces the overall network load.

Security: Edge streaming can enhance security, as sensitive video data remains within the organization's network. It doesn't traverse public internet connections, reducing exposure to potential security threats and unauthorized access.

Scalability: While edge streaming offers low latency and bandwidth efficiency, it may require additional resources, including processing power and storage, at the edge devices. Scalability can be a concern if the network architecture needs to support a large number of cameras or sensors.

2. Cloud Streaming:

Koffka Khan, "A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT)," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

Cloud Streaming, on the other hand, involves sending video data from the edge devices (cameras or sensors) to a central cloud server for processing and storage before being streamed to end-users or devices. This approach offers its own set of advantages and considerations:

Centralized Processing: Cloud streaming allows for centralized video data processing, which can be more powerful and resource-efficient for handling large volumes of video streams. Machine learning and analytics can be applied at scale in the cloud, providing insights and automation.

Flexibility and Remote Access: Cloud streaming offers the advantage of remote access and management. Users can access video feeds from anywhere with an internet connection, making it suitable for applications that require remote monitoring and management.

Data Storage and Redundancy: Cloud storage solutions are typically robust and offer redundancy, ensuring data integrity and availability. This is crucial for applications that require long-term storage, compliance, or historical analysis.

Potential Latency: The downside of cloud streaming is that it introduces latency. Video data must traverse the network to reach the cloud server for processing and storage, which can result in delays. While this may not be critical for all applications, it can impact real-time decision-making.

Security Considerations: Cloud streaming involves transmitting video data over the public internet, which can raise security concerns. Robust encryption and access controls are essential to safeguard the data during transmission and storage in the cloud.

Cost Implications: The cost of cloud streaming can be a consideration, especially for organizations with large numbers of cameras or sensors generating substantial data. Data storage costs, processing fees, and network transfer fees can add up.

In conclusion, the choice between Edge Streaming and Cloud Streaming within the VSIIoT Taxonomy's Network Architecture category depends on the specific requirements and constraints of the IIoT application. Edge Streaming prioritizes low latency and bandwidth efficiency, while Cloud Streaming offers centralized processing, flexibility, and scalability at the expense of potential latency and security considerations. Careful consideration of these factors is crucial to design an effective and efficient video streaming solution in the IIoT landscape.

B. Streaming Protocol [11]:

Real-time Transport Protocol (RTP): A common protocol for streaming real-time multimedia data.

HTTP-based Streaming: Using HTTP-based protocols such as HTTP Live Streaming (HLS) or Dynamic Adaptive Streaming over HTTP (DASH) for video delivery.

Here are some additional details:

Within the Video Streaming in Industrial IoT (VSIIoT) Taxonomy, the choice of streaming protocol is a critical consideration that directly impacts the efficiency, performance, and compatibility of video streaming in industrial applications. This section delves into two primary streaming protocols: Real-time Transport Protocol (RTP) and HTTP-based Streaming, explaining their characteristics and use cases.

1. Real-time Transport Protocol (RTP):

The Real-time Transport Protocol (RTP) is a fundamental protocol widely used in video streaming, especially for real-time multimedia data. It is designed to support the transmission of time-sensitive data, making it suitable for applications that require low latency and real-time delivery of video, such as surveillance, live video feeds, and video conferencing. Key aspects of RTP include:

Real-time Delivery: RTP is optimized for real-time delivery and playback of multimedia data. It prioritizes minimizing latency, making it a preferred choice for applications where timeliness is critical.

Header Information: RTP includes a header that provides essential information about the data, such as timestamp, sequence number, and payload type. This metadata is crucial for synchronizing audio and video streams and ensuring their proper playback.

Scalability: RTP supports multicast transmission, allowing a single video stream to be efficiently delivered to multiple recipients simultaneously. This is advantageous for scenarios like video broadcasting and multi-viewer surveillance.

Codec Agnostic: RTP is codec-agnostic, meaning it can work with a variety of video and audio codecs, offering flexibility in choosing the most suitable codec for the application.

UDP Transport: RTP typically uses the User Datagram Protocol (UDP) for transmission, which offers low overhead but may not guarantee delivery or error correction. Error resilience mechanisms must be implemented at higher layers.

2. HTTP-based Streaming:

HTTP-based streaming protocols, exemplified by technologies like HTTP Live Streaming (HLS) and Dynamic Adaptive Streaming over HTTP (DASH), have gained prominence in recent years, offering several advantages for video delivery in industrial contexts. Here's an in-depth look at HTTP-based streaming:

HTTP Delivery: HTTP-based streaming protocols rely on standard HTTP for data delivery. This makes them compatible with existing web infrastructure and firewalls. Videos are delivered over familiar HTTP ports (e.g., 80 or 443), simplifying network configuration.

Adaptive Streaming: A key strength of HTTP-based streaming is adaptive bitrate streaming (ABR). With ABR, video content is divided into small segments, and different quality versions are created. The streaming client dynamically selects the appropriate quality level based on network conditions, ensuring smooth playback even with varying bandwidth.

Content Protection: HTTP-based streaming protocols offer robust content protection mechanisms. Technologies like Digital Rights Management (DRM) can be integrated to secure video content from unauthorized access and piracy.

Scalability: HTTP-based streaming is highly scalable and can handle a large number of viewers efficiently. Content distribution networks (CDNs) are often used to replicate and distribute video segments to geographically dispersed viewers.

Compatibility: HTTP-based streaming works on a wide range of devices and platforms, including web browsers, mobile devices, and smart TVs. This versatility is valuable for applications that target diverse end-user devices.

Latency Considerations: While HTTP-based streaming is excellent for delivering high-quality video, it may introduce higher latency compared to RTP. This latency can vary based on segment size and ABR settings, which may not be ideal for applications requiring ultra-low latency.

In summary, the choice between RTP and HTTP-based streaming within the VSIIoT Taxonomy's Streaming Protocol category depends on the specific requirements of the industrial video streaming application. RTP excels in low-latency, real-time scenarios, while HTTP-based streaming offers adaptability, compatibility, and content protection mechanisms that are valuable in a broader range of use cases, particularly when delivering video to diverse end-user devices over the public internet.

C. Video Quality and Resolution [2]:

Low-Resolution Streaming: Transmitting lower quality video to conserve bandwidth.

High-Resolution Streaming: Transmitting high-definition video for detailed monitoring.

Here are some additional details:

The quality and resolution of video streams play a pivotal role in determining the effectiveness and suitability of video streaming solutions in industrial applications. Within the Video Streaming in Industrial IoT (VSIIoT) Taxonomy, the distinction between Low-Resolution Streaming and High-Resolution Streaming offers organizations the flexibility to choose the most appropriate quality level for their specific requirements.

1. Low-Resolution Streaming:

Low-Resolution Streaming is the practice of transmitting video with reduced quality to conserve bandwidth and optimize network resources. This approach is characterized by the following key elements:

Bandwidth Efficiency: Low-Resolution Streaming is well-suited for situations where conserving bandwidth is a primary concern. By reducing video quality, less data needs to be transmitted, which is particularly advantageous in networks with limited capacity.

Real-time Performance: In applications where real-time monitoring and rapid decision-making are paramount, such as video surveillance, low-resolution video streams can be transmitted more swiftly. This ensures that critical events are conveyed without significant delay.

Resource Conservation: Devices capturing video, such as cameras or sensors, may have limited processing capabilities. Low-Resolution Streaming reduces the processing and storage demands on these devices, extending their operational life and reducing operational costs.

Scalability: Transmitting lower-resolution video can enhance system scalability. More cameras or sensors can be accommodated on the same network infrastructure without overloading it.

Cost Savings: Reducing video quality often results in cost savings, as less data is transmitted, leading to decreased data transfer and storage expenses.

However, it's essential to acknowledge that Low-Resolution Streaming may not be suitable for applications where high-definition video is imperative, such as situations where detailed visual inspection is required or when evidence quality is necessary for compliance or security purposes.

2. High-Resolution Streaming:

High-Resolution Streaming involves transmitting video in high-definition quality, providing detailed and clear visuals. This approach is characterized by several key attributes:

Detailed Monitoring: High-Resolution Streaming is invaluable in applications that require detailed monitoring, inspection, or analysis. For instance, it's crucial in quality control processes, where fine product details need to be examined.

Enhanced Security: In security and surveillance applications, high-resolution video provides better identification and recognition of individuals or objects, enhancing the effectiveness of video surveillance systems.

Quality Inspection: In manufacturing or industrial processes, high-resolution streaming is often used for quality inspection, enabling the detection of defects or irregularities with precision.

Data-Intensive: High-resolution video requires significantly more bandwidth and storage space. As a result, it's essential to have robust network infrastructure and storage capabilities to support this level of video quality.

Evidentiary Value: In legal or compliance scenarios, high-resolution video can serve as reliable evidence due to its clarity and detail, potentially impacting investigations or audits.

High-Resolution Streaming is ideal for applications where visual quality and detail are critical, even if it results in higher data transfer and storage costs. It is a choice made when the benefits of detailed video outweigh the associated expenses.

In conclusion, the choice between Low-Resolution Streaming and High-Resolution Streaming within the VSIIoT Taxonomy's Video Quality and Resolution category is contingent on the specific requirements and priorities of the industrial application. It involves a trade-off between conserving bandwidth and resources with lower quality video and achieving enhanced visual quality and detail with high-resolution video, based on the application's objectives and constraints.

D. Latency [16]:

Low-Latency Streaming: Minimizing the delay between capturing and displaying video data.

High-Latency Streaming: Accepting some delay for improved video quality and reliability.

Here are the component details:

Latency, the delay between capturing and displaying video data, is a critical factor in the effectiveness of video streaming solutions in industrial applications. In the Video Streaming in Industrial IoT (VSIIoT) Taxonomy, the distinction between Low-Latency Streaming and High-Latency Streaming offers organizations the flexibility to choose the most suitable latency level for their specific needs.

1. Low-Latency Streaming:

Koffka Khan, "A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT)," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

Low-Latency Streaming prioritizes minimizing the delay between capturing video data and displaying it to end-users or devices. This approach offers several important advantages:

Real-Time Monitoring: Low-latency streaming is essential for applications that require real-time monitoring, such as video surveillance, remote control of industrial processes, and teleoperation. It ensures that the video feed is as close to real-time as possible, enabling immediate decision-making and response to events.

Interactive Communication: In applications where video interaction is involved, such as video conferencing or remote assistance, low-latency streaming is crucial for maintaining natural conversations and interactions.

Safety and Security: In security and safety-critical applications, low-latency video is essential to provide timely alerts and actions. For example, in critical infrastructure protection, a low-latency video stream can help prevent and respond to security breaches swiftly.

Edge Computing: Low-latency streaming often aligns with edge computing, where data processing occurs closer to the data source. Edge computing reduces the time taken for data to traverse the network and provides faster insights.

Real-time Data Synchronization: For applications that require synchronization between video data and other real-time data sources, such as sensor data, low-latency streaming is crucial to ensure timely correlation and analysis.

However, achieving low latency can be challenging and may require dedicated network infrastructure, optimized processing at the edge, and efficient compression techniques. It's also worth noting that achieving extremely low latency may come at the expense of video quality.

2. High-Latency Streaming:

High-Latency Streaming, on the other hand, accepts a certain degree of delay between video capture and display in exchange for improved video quality, reliability, or other benefits. This approach has its own set of use cases and considerations:

Enhanced Video Quality: High-latency streaming allows for the transmission of higher-quality video, including high-resolution and less compressed formats. This is advantageous when the visual detail is of paramount importance, such as in quality control or fine inspection processes.

Network Resilience: In less stable or reliable network environments, a higher-latency approach can provide better resilience. It allows for buffering and error correction mechanisms, ensuring that video playback remains smooth even in challenging network conditions.

Resource Optimization: High-latency streaming can reduce the processing and network demands on edge devices, which may be beneficial for resource-constrained devices. It can also enable better scalability, as video processing and distribution can be managed centrally.

Data Analysis: In scenarios where video data needs to be analyzed or post-processed before being used, accepting some latency can provide more time for in-depth analysis, potentially leading to better insights.

High-latency streaming is often used in scenarios where video quality, reliability, and data analysis are the primary considerations, and immediate real-time monitoring is not essential.

In conclusion, the choice between Low-Latency Streaming and High-Latency Streaming within the VSIIoT Taxonomy's Latency category hinges on the specific requirements and priorities of the industrial application. It involves a trade-off between minimizing delay for real-time monitoring and interactions or accepting some latency for improved video quality, reliability, and resource optimization, depending on the application's objectives and network conditions.

E. Camera Type [14]:

Fixed Cameras: Stationary cameras capturing specific areas continuously.

Pan-Tilt-Zoom (PTZ) Cameras: Adjustable cameras for remote control and monitoring.

360-Degree Cameras: Cameras that capture panoramic views of an area.

Here are further details:

In the realm of video streaming within the Industrial Internet of Things (IIoT), the type of camera used is a crucial determinant of the video capture and monitoring capabilities. The Video Streaming in Industrial IoT (VSIIoT) Taxonomy classifies cameras into three primary categories: Fixed Cameras, Pan-Tilt-Zoom (PTZ) Cameras, and 360-Degree Cameras, each designed for specific use cases and offering distinct advantages.

1. Fixed Cameras:

Fixed Cameras, as the name suggests, are stationary devices that capture specific areas continuously without the ability to adjust their field of view. These cameras offer several important features and are particularly well-suited for certain applications:

Consistent Monitoring: Fixed cameras provide consistent and unchanging views of predefined areas, making them ideal for continuous surveillance, monitoring, and recording. They are often deployed in settings where specific areas need constant observation, such as entrances, production lines, or critical infrastructure locations.

Cost-Effective: Fixed cameras are often more cost-effective than their adjustable counterparts, making them a practical choice for organizations with budget constraints or the need for multiple cameras to cover various locations.

Ease of Setup: These cameras are typically easier to install and set up since they require minimal configuration and calibration. This ease of deployment makes them an attractive option for applications that demand quick implementation.

Reliability: Fixed cameras are known for their reliability since there are fewer moving parts and variables involved. They are less susceptible to mechanical wear and tear, which is crucial in industrial environments.

While fixed cameras excel in providing consistent monitoring of specific areas, they are limited by their inability to adapt to changing conditions or zoom in for closer inspection. They are not suitable for scenarios where dynamic monitoring, remote control, or panoramic views are required.

2. Pan-Tilt-Zoom (PTZ) Cameras:

Pan-Tilt-Zoom (PTZ) Cameras are adjustable cameras designed for remote control and monitoring. These cameras

Koffka Khan, "A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT)," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

offer a broad range of features and benefits, making them valuable for various applications:

Adjustable Field of View: PTZ cameras can pan, tilt, and zoom, allowing users to remotely adjust their field of view. This adaptability is advantageous for tracking moving objects, zooming in for detail, or surveying larger areas.

Dynamic Monitoring: PTZ cameras offer dynamic and responsive monitoring capabilities, making them suitable for applications that require tracking and following subjects or events in real time. They can cover a wide area with a single camera.

Optical Zoom: These cameras often come with optical zoom capabilities, providing high-quality zoomed-in images without sacrificing image quality, which is vital in applications like license plate recognition or facial recognition.

Presets and Tours: Many PTZ cameras support preset positions and automated tours, allowing them to switch between predefined locations and viewpoints. This feature is useful for routine inspections or surveillance.

Remote Control: PTZ cameras can be controlled remotely through software interfaces or physical controllers, providing users with the ability to adjust the camera's position and zoom as needed.

Despite their versatility and dynamic monitoring capabilities, PTZ cameras tend to be more complex to set up and maintain compared to fixed cameras. They are an excellent choice when adaptability, remote control, and close-up inspection are required.

3. 360-Degree Cameras:

360-Degree Cameras, also known as panoramic cameras, are designed to capture a complete view of their surroundings in all directions. These cameras offer unique advantages for specific use cases:

Comprehensive Coverage: 360-degree cameras capture a panoramic view of an area without any blind spots. This comprehensive coverage is especially valuable in applications where a complete view is required, such as large open spaces, retail environments, or traffic monitoring.

Simplified Installation: Due to their ability to capture a wide area, fewer cameras are needed to cover the same space compared to fixed or PTZ cameras. This can result in cost savings on camera hardware and installation.

Situational Awareness: 360-degree cameras enhance situational awareness by providing a complete view of an area. This is particularly useful in surveillance and security applications, allowing operators to monitor and respond to events more effectively.

Immersive Experience: These cameras are suitable for applications that aim to create an immersive experience, such as virtual tours, augmented reality, or immersive video conferencing.

However, 360-degree cameras have limitations in terms of detailed zooming and tracking moving objects, as their focus is on providing an overall view rather than close-ups or dynamic monitoring.

In conclusion, the choice of camera type within the VSIIoT Taxonomy's Camera Type category should align with the specific requirements of the industrial application. Fixed cameras are ideal for continuous monitoring of specific areas, PTZ cameras provide adaptability and dynamic monitoring, and 360-degree cameras offer complete coverage for immersive experiences and comprehensive surveillance. The decision should be based on the application's needs for coverage, adaptability, and zoom capabilities, as well as budget considerations.

F. Security and Authentication [1]:

Secure Streaming: Employing encryption and authentication mechanisms to protect video data from unauthorized access.

Non-Secure Streaming: Transmitting video without advanced security measures.

In the Video Streaming in Industrial IoT (VSIIoT) Taxonomy, the category of Security and Authentication is a pivotal consideration when implementing video streaming solutions. This classification encompasses two primary approaches: Secure Streaming and Non-Secure Streaming, each of which has distinct features and implications for safeguarding video data in industrial applications.

1. Secure Streaming:

Secure Streaming involves the implementation of robust security measures, including encryption and authentication mechanisms, to protect video data from unauthorized access, tampering, and interception. The key aspects and benefits of Secure Streaming include:

Data Encryption: Secure Streaming typically employs encryption to ensure that video data is transmitted in an unreadable format. This encryption can encompass data at rest (when stored) and data in transit (when transmitted over networks). Advanced encryption standards, such as AES (Advanced Encryption Standard), are commonly used to secure video streams.

Authentication: Secure Streaming uses authentication mechanisms to verify the identity of both the sender and the receiver of video data. User authentication ensures that only authorized individuals or devices can access and view the video streams. Multi-factor authentication can add an extra layer of security.

Access Control: Secure Streaming solutions provide fine-grained control over who can access the video streams, where they can be accessed from, and what actions users are allowed to perform (e.g., viewing, recording, or controlling PTZ cameras). Access control policies are enforced to restrict unauthorized access.

Data Integrity: To prevent data tampering and ensure data integrity, Secure Streaming incorporates mechanisms for detecting and verifying the authenticity of video data. Digital signatures and integrity checks are used to ensure that the data has not been altered during transmission.

Compliance: Secure Streaming aligns with industry and regulatory standards for data protection, privacy, and security. This is crucial for applications that must adhere to strict compliance requirements, such as those in healthcare, finance, or critical infrastructure.

Protection Against Eavesdropping: Secure Streaming safeguards video data from eavesdropping and interception by

Koffka Khan, “A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT),” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

unauthorized third parties. This is essential in scenarios where confidentiality and privacy are paramount.

Secure Streaming is highly recommended for industrial applications where the security and privacy of video data are critical, such as surveillance, critical infrastructure protection, or applications dealing with sensitive information. However, implementing secure streaming may involve additional costs and complexity in terms of security infrastructure and key management.

2. Non-Secure Streaming:

Non-Secure Streaming, in contrast, involves transmitting video data without employing advanced security measures, such as encryption and strong authentication. This approach may be employed in situations where security is of lower concern, or the specific use case does not warrant the added complexity and costs associated with secure streaming. Key aspects and considerations of Non-Secure Streaming include:

Simplicity and Cost: Non-Secure Streaming is generally simpler to set up and operate. It can be a cost-effective choice for applications that prioritize simplicity and have minimal security requirements.

Low Overhead: The absence of encryption and complex authentication mechanisms results in lower computational overhead, which may be advantageous for resource-constrained devices or networks.

Non-Confidential Data: Non-Secure Streaming is suitable for scenarios where the video content is non-confidential, non-sensitive, or intended for public consumption. Examples may include live streaming of public events or marketing purposes.

However, Non-Secure Streaming should be avoided in applications where video data contains sensitive or confidential information, as it leaves data vulnerable to interception, tampering, and unauthorized access. It is also not suitable for applications that must adhere to regulatory or compliance standards that require data protection.

In conclusion, the choice between Secure Streaming and Non-Secure Streaming within the VSIIoT Taxonomy's Security and Authentication category should be determined by the specific security requirements and compliance obligations of the industrial application. Secure Streaming is essential when confidentiality, privacy, and regulatory compliance are paramount, while Non-Secure Streaming may be appropriate for scenarios with lower security concerns and a focus on simplicity and cost-effectiveness.

G. Use Cases [19]:

Surveillance and Security: Monitoring and securing critical infrastructure and assets.

Predictive Maintenance: Using video data for machine health analysis and fault prediction.

Process Monitoring: Monitoring industrial processes to optimize efficiency and quality.

Quality Control: Inspecting products for defects in manufacturing.

Here are further details:

Use Cases represent the practical applications of video streaming within the Industrial Internet of Things (IIoT) ecosystem. The Video Streaming in Industrial IoT (VSIIoT) Taxonomy categorizes these applications into specific areas, each with its unique objectives and benefits. Let's explore four prominent Use Cases within the VSIIoT Taxonomy:

1. Surveillance and Security:

Overview: Surveillance and Security is a fundamental use case that involves the monitoring and safeguarding of critical infrastructure, assets, and facilities. This application leverages video streaming technology to enhance security, deter threats, and respond to security incidents.

Key Aspects:

Continuous Monitoring: Video streams from cameras are continuously monitored to detect unauthorized access, security breaches, and suspicious activities.

Event Recognition: Advanced analytics and AI-powered algorithms can be applied to video data to recognize specific events, such as intrusions, trespassing, or unattended packages.

Alarm and Notification: Surveillance and Security systems are equipped with alerting mechanisms, enabling the immediate notification of security personnel or first responders when security incidents are detected.

Deterrence: Visible cameras act as a deterrent to potential intruders and wrongdoers, enhancing the security posture of the monitored area.

Evidence Collection: Video footage serves as evidence for investigating security incidents, identifying suspects, and addressing legal or compliance requirements.

Access Control: Video streams can be integrated with access control systems, allowing security personnel to verify the identity of individuals and grant or deny access.

Surveillance and Security is crucial for protecting critical infrastructure, such as power plants, transportation hubs, and sensitive manufacturing facilities, as well as for general safety and public spaces.

2. Predictive Maintenance:

Overview: Predictive Maintenance employs video data for machine health analysis and fault prediction. By monitoring machinery and equipment through video streams, organizations can prevent unexpected failures and reduce downtime.

Key Aspects:

Condition Monitoring: Video streams are used to assess the condition of machines and equipment, identifying signs of wear, damage, or anomalies.

Anomaly Detection: Machine learning algorithms can analyze video data to identify subtle changes or irregularities in machine behavior, which may indicate impending failures.

Predictive Analytics: The insights derived from video data enable organizations to predict when maintenance is required, reducing unplanned downtime and increasing operational efficiency.

Cost Reduction: Predictive Maintenance can significantly reduce maintenance costs by shifting from reactive maintenance (fixing after failure) to proactive maintenance (preventing failures).

Equipment Longevity: By proactively addressing issues, organizations can extend the lifespan of their machinery and equipment, optimizing their investments.

Koffka Khan, "A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT)," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

Predictive Maintenance is instrumental in industries where machinery and equipment downtime can lead to significant production losses and costs, such as manufacturing, energy, and transportation.

3. Process Monitoring:

Overview: Process Monitoring focuses on the real-time observation and analysis of industrial processes to optimize efficiency, quality, and compliance with standards. Video streaming technology is used to gain insights into process operations.

Key Aspects:

Real-Time Observations: Video feeds from cameras provide real-time insights into manufacturing processes, chemical reactions, or assembly lines.

Quality Assurance: Process Monitoring enables the detection of defects, deviations, or irregularities in product manufacturing, allowing for immediate intervention to maintain product quality.

Process Optimization: The data derived from video streams can be used to optimize processes, improve workflow, and identify opportunities for efficiency gains.

Compliance: In regulated industries, Process Monitoring ensures adherence to industry standards, quality control, and environmental regulations.

Documentation: Video streams serve as valuable documentation for process auditing, compliance, and continuous improvement initiatives.

Process Monitoring is vital in industries where precise control of operations and product quality is essential, such as pharmaceuticals, food production, and chemical manufacturing.

4. Quality Control:

Overview: Quality Control employs video streaming technology for inspecting products and components to identify defects, anomalies, or imperfections during manufacturing or assembly processes.

Key Aspects:

Visual Inspection: High-resolution video streams provide detailed visual data for quality assessment.

Automated Inspection: Machine vision and computer vision systems can automate the inspection process, flagging defects and anomalies.

Defect Recognition: AI algorithms can be trained to recognize specific defects, ensuring consistent and accurate defect identification.

Sorting and Rejection: Products failing quality control standards can be automatically sorted or rejected, ensuring only high-quality products reach the market.

Data Logging: Quality Control systems log and store inspection data for traceability and quality assurance.

Quality Control is indispensable in industries where product defects can have significant consequences, such as automotive manufacturing, electronics, and consumer goods production.

In summary, the VSIIoT Taxonomy's Use Cases classification encompasses a range of practical applications for video streaming in industrial contexts. These applications, including Surveillance and Security, Predictive Maintenance, Process Monitoring, and Quality Control, address specific needs, ranging from security and safety to operational efficiency and product quality. The choice of a use case depends on the objectives and priorities of the organization or industry.

H. Integration with Other IIoT Technologies:

Sensor Integration: Combining video data with sensor data for more comprehensive insights.

Cloud Integration [21]: Incorporating video streams into broader IIoT cloud-based platforms.

Here are further details:

The integration of video streaming with other IIoT technologies is a crucial aspect of modern industrial operations. It allows for more comprehensive data insights, enhanced decision-making, and the optimization of various processes. In the Video Streaming in Industrial IoT (VSIIoT) Taxonomy, two significant integration approaches are highlighted: Sensor Integration and Cloud Integration.

1. Sensor Integration:

Overview: Sensor Integration refers to the combination of video data with data from various sensors within the IIoT ecosystem. This integration creates a more holistic view of industrial processes, assets, and environments. Key aspects and benefits of Sensor Integration include:

Comprehensive Data Insights: By combining video data with sensor data, organizations gain a more complete understanding of what is happening in their industrial environments. This comprehensive data can reveal correlations, anomalies, and insights that would be challenging to discover with either video or sensor data alone.

Cross-Verification: Video data can be used to validate or complement sensor readings. For example, a temperature sensor in a manufacturing facility can be cross-verified by visual inspection via video to ensure that the equipment is operating within specified parameters.

Contextualization: Video data provides context to sensor data, making it easier to interpret and act upon. For instance, video can help explain why a sensor detected an anomaly by showing a visual representation of the situation.

Visual Monitoring: Sensors can trigger video recording or alerts based on specific sensor conditions. For example, if a motion sensor detects an unauthorized intrusion, it can activate a video camera to provide visual evidence.

Predictive Maintenance: Combining sensor and video data enables predictive maintenance models to analyze both machine condition and visible signs of wear or damage, leading to more accurate maintenance predictions.

Quality Control: Sensor data can help identify parameters that affect product quality, while video data can provide visual inspection for quality assurance, improving quality control processes.

Sensor Integration is particularly valuable in industries where both sensor and visual data are integral to operations, such as manufacturing, agriculture, and environmental monitoring. It helps organizations make data-driven decisions, optimize processes, and enhance safety and quality.

2. Cloud Integration:

Koffka Khan, “A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT),” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

Overview: Cloud Integration involves the incorporation of video streams into broader IIoT cloud-based platforms. Cloud platforms provide scalable, flexible, and centralized solutions for managing, analyzing, and storing video data. Key aspects and advantages of Cloud Integration include:

Centralized Data Management: Cloud platforms centralize video data, making it accessible from anywhere with an internet connection. This is beneficial for organizations with multiple locations or remote operations.

Scalability: Cloud-based solutions are highly scalable, allowing organizations to accommodate a growing number of cameras and streams without the need for extensive on-site infrastructure.

Data Analytics: Cloud platforms often include powerful analytics and machine learning capabilities, enabling organizations to gain deeper insights from video data, detect anomalies, and derive valuable business intelligence.

Remote Access: Authorized personnel can access video streams and analytics from anywhere, providing flexibility for remote monitoring and management.

Data Storage and Redundancy: Cloud platforms offer robust data storage and redundancy options, ensuring that video data is securely preserved and available when needed.

Security: Cloud platforms often come with advanced security features, including encryption, access controls, and identity management, ensuring the confidentiality and integrity of video data.

Collaboration: Cloud-based platforms facilitate collaboration and data sharing among different departments or external partners, enhancing situational awareness and decision-making.

Cloud Integration is especially advantageous for organizations seeking to leverage the power of the cloud for centralized data management, advanced analytics, and remote access. It is relevant in various industries, including logistics, retail, and smart city applications.

In summary, the VSIIoT Taxonomy's Integration with Other IIoT Technologies category emphasizes the importance of combining video streaming with other data sources and cloud platforms to maximize the value and insights gained from industrial operations. Sensor Integration provides a more comprehensive view of industrial processes and assets, while Cloud Integration offers scalability, analytics, and centralized management of video data. The choice of integration approach depends on the specific requirements, scale, and objectives of the industrial application.

I. Data Storage [2]:

Real-time Streaming: Discarding video data after real-time analysis without saving it.

Video Recording: Storing video data for historical analysis, compliance, or evidence.

Data storage is a critical aspect of video streaming in the context of the Industrial Internet of Things (IIoT). The Video Streaming in Industrial IoT (VSIIoT) Taxonomy classifies data storage into two primary approaches: Real-time Streaming and Video Recording, each serving distinct purposes and offering specific benefits.

1. Real-time Streaming:

Overview: Real-time Streaming involves the practice of discarding video data immediately after real-time analysis and viewing, without retaining it for future reference or historical analysis. This approach is often favored in scenarios where real-time insights and immediate decision-making are the primary objectives.

Key Aspects:

Low Latency: Real-time streaming prioritizes minimal latency, ensuring that video data is processed and delivered as quickly as possible. This is crucial for applications that require rapid responses to events, such as surveillance and live monitoring.

Reduced Storage Requirements: By not retaining video data, real-time streaming reduces the need for extensive data storage infrastructure. This can result in cost savings and simplified data management.

Privacy and Data Protection: Since video data is not stored, there is a reduced risk of data breaches, unauthorized access, or privacy concerns, making this approach suitable for applications with stringent data protection requirements.

Use Cases:

Surveillance and Security: Real-time streaming is highly beneficial in security applications where immediate action is required upon event detection, such as unauthorized access or intrusions.

Teleoperation: Remote control of machinery or equipment in real time, such as in telemedicine or teleoperated robots.

Real-time Quality Control: Applications that require immediate detection and correction of production defects.

2. Video Recording:

Overview: Video Recording entails the practice of storing video data for historical analysis, compliance, evidence, and various post-processing purposes. This approach is suitable for applications where long-term data retention and historical insights are essential.

Key Aspects:

Historical Analysis: Video recordings provide a wealth of historical data for post-event analysis, process optimization, and trend identification. This can be valuable for continuous improvement and decision-making.

Compliance and Evidence: Video recordings serve as evidence in legal or compliance-related matters, including investigations, audits, and regulatory requirements.

Data Integrity: Recorded video data can be used to verify the accuracy of sensor data, incidents, and events. It can also help reconstruct the sequence of events for post-incident analysis.

Training and Education: Video recordings are valuable for training, education, and knowledge sharing, allowing organizations to create instructional materials or conduct post-mortem reviews.

Data Preservation: Video recording ensures data preservation for future reference and compliance with data retention policies or industry standards.

Use Cases:

Predictive Maintenance: Historical video data can be used to analyze equipment behavior over time and improve predictive maintenance models.

Koffka Khan, “A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT),” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

Quality Control and Process Monitoring: Retained video data helps in tracking process deviations, identifying quality issues, and optimizing processes.

Logistics and Supply Chain Management: Video recordings can be used for supply chain traceability and incident investigation.

In conclusion, the choice between Real-time Streaming and Video Recording within the VSIIoT Taxonomy's Data Storage category should be based on the specific requirements and objectives of the industrial application. Real-time Streaming is ideal for applications where immediate action and minimal latency are essential, while Video Recording is valuable when historical analysis, compliance, evidence, and long-term data retention are key priorities. The decision should align with the organization's goals and operational needs.

J. Analytics and Machine Learning [12]:

On-the-fly Analytics: Analyzing video data in real-time for immediate decision-making.

Post-processing Analytics: Applying machine learning and analytics to stored video data for insights and trends.

Here are further details:

The integration of analytics and machine learning with video streaming data is pivotal in extracting valuable insights and driving informed decision-making in the Industrial Internet of Things (IIoT) landscape. The Video Streaming in Industrial IoT (VSIIo) Taxonomy classifies this integration into two primary approaches: On-the-fly Analytics and Post-processing Analytics, each offering specific benefits and use cases.

1. On-the-fly Analytics:

Overview: On-the-fly Analytics refers to the real-time analysis of video data as it is being streamed, enabling immediate decision-making based on the insights extracted. This approach is particularly valuable for applications where rapid response and situational awareness are of paramount importance.

Key Aspects:

Real-time Decision-Making: On-the-fly analytics enables organizations to make immediate decisions based on live video data. This is essential for scenarios where swift responses are required, such as security, safety, or process control.

Event Detection: Real-time analytics can detect specific events, anomalies, or patterns as they occur, triggering automated actions or alerts. For example, it can detect unauthorized access, equipment faults, or process deviations in real time.

Low Latency: On-the-fly analytics emphasizes low latency, ensuring that insights are derived and acted upon with minimal delay. This is crucial for maintaining situational awareness and responding to events promptly.

Dynamic Adaptation: Real-time analytics can adapt to changing conditions, enabling organizations to modify algorithms or rules based on the evolving environment or requirements.

Live Monitoring: On-the-fly analytics is well-suited for live monitoring applications, where operators need to track and respond to events as they unfold.

Use Cases:

Security and Surveillance: Real-time analytics are used to detect intrusions, unusual behaviors, or security breaches in real time, enhancing the effectiveness of security systems.

Manufacturing Process Control: On-the-fly analytics help monitor and control industrial processes, ensuring that production remains within specified parameters.

Healthcare Monitoring: In telemedicine and remote healthcare applications, real-time analytics can monitor patient conditions, detect anomalies, and trigger alerts to medical professionals.

2. Post-processing Analytics:

Overview: Post-processing Analytics involves the application of machine learning, artificial intelligence, and advanced analytics to stored video data for retrospective analysis, insights, and trend identification. This approach is valuable for applications that require historical data-driven decision-making, process optimization, or compliance.

Key Aspects:

Historical Analysis: Post-processing analytics leverages historical video data to identify trends, anomalies, and patterns over time. This allows organizations to make data-driven decisions and optimizations based on historical insights.

Predictive Insights: Analyzing archived video data can lead to the development of predictive models for events or outcomes, helping organizations anticipate issues or opportunities.

Compliance and Auditing: Post-processing analytics is used to ensure compliance with industry standards, regulations, and auditing requirements by reviewing historical data for incidents or anomalies.

Training and Education: Insights from post-processing analytics can be used for training, knowledge sharing, or creating instructional materials based on historical data.

Continuous Improvement: Organizations can use post-processing analytics to continuously improve processes, enhance product quality, and optimize operations based on historical analysis.

Use Cases:

Predictive Maintenance: Post-processing analytics can analyze historical video data to predict equipment failures and optimize maintenance schedules.

Quality Control and Process Optimization: Retrospective analysis of video data helps identify trends, defects, and process improvements for quality control and efficiency.

Retail and Customer Analytics: In retail, post-processing analytics can provide insights into customer behavior, buying patterns, and store optimization.

In summary, the choice between On-the-fly Analytics and Post-processing Analytics within the VSIIoT Taxonomy's Analytics and Machine Learning category should align with the specific objectives and operational requirements of the industrial application. On-the-fly Analytics is ideal for real-time decision-making and immediate response, while Post-processing Analytics is valuable for retrospective analysis, historical insights, and continuous improvement. The decision should be driven by the organization's goals and the nature of the application.

K. Scalability [18]:

Scalable Streaming: Systems that can accommodate an increasing number of cameras and users.

Non-Scalable Streaming: Limited in terms of camera or user capacity.

Here’s further details:

Scalability is a crucial aspect of video streaming within the context of the Industrial Internet of Things (IIoT). The Video Streaming in Industrial IoT (VSIIoT) Taxonomy categorizes scalability into two primary approaches: Scalable Streaming and Non-Scalable Streaming, each with distinct implications for accommodating the growing number of cameras and users in industrial applications.

1. Scalable Streaming:

Overview: Scalable Streaming refers to video streaming systems designed to accommodate an increasing number of cameras, users, or devices without significant degradation in performance or the need for substantial infrastructure changes. Scalability is vital in dynamic industrial environments where expansion is expected.

Key Aspects:

Flexible Infrastructure: Scalable streaming solutions are designed with a flexible infrastructure that can be easily expanded to accommodate additional cameras, sensors, and users as the need arises.

Load Distribution: These systems can distribute the load efficiently across the network, servers, and storage, ensuring that the performance remains consistent even with a larger number of video streams.

Adaptive Network Design: Scalable streaming solutions often use adaptive network designs that can handle increased data traffic and bandwidth requirements, reducing the risk of network congestion or slowdowns.

Resource Optimization: These systems are resource-efficient, making the most of available hardware and software resources to maintain performance while scaling up.

User Access Control: Scalable streaming platforms include user access controls and permissions to manage a growing user base while maintaining data security.

Use Cases:

Smart Cities: Scalable streaming is crucial for urban surveillance systems that need to expand to cover more areas and support more cameras as the city grows.

Large-Scale Manufacturing: In manufacturing environments, scalable streaming supports the addition of cameras and sensors in response to changing production demands.

Logistics and Warehousing: As warehouses expand or new facilities are added, scalable streaming ensures that surveillance and monitoring systems can adapt to the increased size.

2. Non-Scalable Streaming:

Overview: Non-Scalable Streaming, in contrast, refers to video streaming systems that have limitations in terms of camera or user capacity. These systems may struggle to maintain performance and user experience when the number of cameras or users exceeds a certain threshold.

Key Aspects:

Fixed Capacity: Non-scalable streaming systems have a fixed capacity, often defined during their initial design and implementation. When this capacity is reached, the system may experience performance issues.

Infrastructure Overhead: Expanding a non-scalable system typically requires a substantial investment in infrastructure changes, which can be costly and time-consuming.

Risk of Bottlenecks: Non-scalable systems are more susceptible to network bottlenecks, data congestion, and decreased performance as the number of cameras and users grows.

Limited Adaptability: Non-scalable systems may struggle to adapt to changes in operational requirements, leading to operational inefficiencies or constraints.

Use Cases:

Small-Scale Operations: Non-scalable streaming may be sufficient for smaller operations with a fixed number of cameras and a limited user base.

Static Environments: Applications in static environments, where camera and user requirements remain constant, can often work with non-scalable solutions.

Cost-Constrained Scenarios: Non-scalable streaming may be preferred in scenarios with budget constraints, where the cost of upgrading infrastructure for scalability is prohibitive.

In conclusion, the choice between Scalable Streaming and Non-Scalable Streaming within the VSIIoT Taxonomy's Scalability category should be determined by the specific requirements, expected growth, and operational constraints of the industrial application. Scalable Streaming is ideal for dynamic environments that require flexibility, adaptability, and the ability to accommodate a growing number of cameras and users. Non-Scalable Streaming, on the other hand, is suited for static or small-scale operations where scalability is not a priority or where budget constraints limit infrastructure expansion. The decision should align with the organization's objectives and operational needs.

L. Regulatory Compliance:

Compliance-Oriented Streaming: Meeting specific industry or regional regulations for video data.

Here’s further details:

Regulatory compliance is a critical consideration in the implementation of video streaming within the Industrial Internet of Things (IIoT) landscape. The Video Streaming in Industrial IoT (VSIIoT) Taxonomy categorizes regulatory compliance into Compliance-Oriented Streaming, focusing on the importance of adhering to industry or regional regulations for video data.

1. Compliance-Oriented Streaming:

Overview: Compliance-Oriented Streaming refers to the practice of aligning video streaming systems with specific industry or regional regulations and standards governing the collection, storage, transmission, and use of video data. This approach is essential in industries and applications where regulatory compliance is mandated and non-compliance can result in legal, financial, or reputational consequences.

Koffka Khan, “A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT),” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

Key Aspects:

Regulatory Alignment: Compliance-oriented streaming systems are designed and configured to align with the applicable regulations, standards, and requirements governing video data usage. This may include industry-specific standards, data protection regulations, privacy laws, and regional mandates.

Data Security and Encryption: To meet regulatory requirements, these systems often incorporate robust data security measures, including encryption for data at rest and in transit. This ensures the confidentiality and integrity of video data.

Access Control and Authentication: Compliance-oriented streaming systems implement strict access control and authentication mechanisms to ensure that only authorized individuals or entities can access and manage video data, in accordance with regulatory requirements.

Data Retention Policies: Many regulations specify data retention periods and requirements. Compliance-oriented systems adhere to these policies, ensuring that video data is retained for the necessary duration and deleted when required.

Audit Trails and Reporting: These systems often include features for generating audit trails and reports to demonstrate compliance with regulations. This is critical for regulatory audits and investigations.

Consent and Privacy: Compliance-oriented streaming systems may incorporate mechanisms for obtaining user consent, especially in applications involving personal or sensitive data. This ensures compliance with data protection and privacy regulations.

Use Cases:

Healthcare: In healthcare applications, compliance-oriented streaming is essential to adhere to the Health Insurance Portability and Accountability Act (HIPAA) in the United States, or similar data protection regulations in other regions, to ensure patient data privacy and security.

Financial Services: In the financial sector, compliance-oriented streaming is necessary to meet regulations such as the Payment Card Industry Data Security Standard (PCI DSS) for securing financial transactions and cardholder data.

Public Safety and Law Enforcement: In law enforcement and public safety applications, compliance-oriented streaming ensures adherence to legal requirements for evidence collection, chain of custody, and privacy.

GDPR and Data Protection: Organizations operating in regions subject to the General Data Protection Regulation (GDPR) in the European Union must adopt compliance-oriented streaming to safeguard the rights and privacy of individuals.

In conclusion, the choice of Compliance-Oriented Streaming within the VSIIoT Taxonomy's Regulatory Compliance category is critical for organizations and applications subject to industry or regional regulations and standards. Compliance-oriented streaming ensures that video data is collected, stored, and transmitted in full accordance with the law and regulatory requirements, mitigating legal and reputational risks. The decision to adopt this approach should be based on the specific regulatory environment in which the organization operates and the consequences of non-compliance.

M. User Access:

Remote Access: Allowing authorized users to view video feeds from anywhere.

Local Access: Restricting video streaming to a local network or physical proximity.

Here’s further details on this taxonomy component:

User access control is a fundamental consideration in the context of video streaming within the Industrial Internet of Things (IIoT). The Video Streaming in Industrial IoT (VSIIoT) Taxonomy classifies user access control into two primary approaches: Remote Access and Local Access, each of which offers distinct benefits and considerations.

1. Remote Access:

Overview: Remote Access allows authorized users to view video feeds from anywhere with an internet connection. This approach provides flexibility and convenience by enabling remote monitoring and management of video streams, which is particularly valuable in applications where real-time access and situational awareness are essential.

Key Aspects:

Global Accessibility: Authorized users can access video feeds from remote locations, providing the ability to monitor and respond to events in real time, regardless of physical proximity to the monitored site.

Mobile and Remote Devices: Remote access supports viewing on various devices, including smartphones, tablets, laptops, and desktop computers, allowing users to stay connected and make informed decisions on the go.

Flexibility: Remote access is well-suited for applications that require continuous monitoring and remote management, such as security, surveillance, and telemedicine.

Scalability: Remote access can accommodate a distributed user base, including personnel at multiple locations, contractors, and third-party service providers.

Cloud Integration: Remote access often integrates with cloud-based platforms, enabling secure and centralized management of video streams and user access control.

Use Cases:

Surveillance and Security: Remote access is crucial for security and surveillance applications where real-time situational awareness and incident response are critical.

Telemedicine and Remote Healthcare: In telemedicine, remote access allows healthcare providers to monitor patients' conditions and provide guidance from a distance.

Cross-Site Monitoring: Organizations with multiple sites or facilities benefit from remote access to centrally manage and monitor video streams across locations.

2. Local Access:

Overview: Local Access restricts video streaming to a local network or physical proximity to the cameras or video sources. This approach enhances security by limiting access to authorized personnel within the premises, but it may reduce flexibility compared to remote access.

Key Aspects:

Enhanced Security: Local access minimizes exposure to external threats by confining access to the local network,

Koffka Khan, “A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT),” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

making it suitable for applications where security and privacy are paramount.

Physical Proximity: Users must be physically present within the local network or facility to access video streams, ensuring that only authorized personnel can view the feeds.

Air-Gapped Environments: Local access is used in secure, air-gapped environments where external network connectivity is restricted for security reasons.

Reduced Network Traffic: Local access limits video streaming traffic to the local network, reducing the load on external network connections.

Compliance: Some industries and applications with stringent regulatory requirements may opt for local access to meet data security and privacy standards.

Use Cases:

Secure Facilities: Local access is crucial for applications in high-security environments, such as government facilities, data centers, and military installations.

Privacy-Sensitive Areas: Local access is used in settings where privacy concerns dictate limited access, such as healthcare facilities, educational institutions, and corporate boardrooms.

Manufacturing and Industrial Control: In industrial environments, local access ensures that video streams are accessible only within the operational facility to prevent external threats.

In summary, the choice between Remote Access and Local Access within the VSIIoT Taxonomy's User Access category should be based on the specific requirements, security considerations, and operational needs of the industrial application. Remote Access provides flexibility and real-time monitoring from anywhere, while Local Access enhances security and is suitable for applications where physical presence and privacy are paramount. The decision should align with the organization's objectives and the nature of the application.

N. Cost and Budget:

High-Cost Solutions: Investing in advanced and robust video streaming systems.

Low-Cost Solutions: Opting for cost-effective video streaming solutions.

Here’s details of this taxonomy component:

Cost and budget considerations play a significant role in the selection and implementation of video streaming systems within the Industrial Internet of Things (IIoT) ecosystem. The Video Streaming in Industrial IoT (VSIIoT) Taxonomy categorizes cost and budget considerations into two primary approaches: High-Cost Solutions and Low-Cost Solutions, each with its own set of implications and trade-offs.

1. High-Cost Solutions:

Overview: High-Cost Solutions involve investing in advanced and robust video streaming systems that offer a comprehensive set of features, capabilities, and high-quality performance. These solutions are characterized by their substantial initial investments and ongoing operational expenses, but they often deliver superior performance and advanced features.

Key Aspects:

Advanced Features: High-cost solutions typically offer advanced features such as high-resolution streaming, low latency, analytics, machine learning integration, and scalability to meet complex and demanding industrial requirements.

Reliability and Redundancy: These solutions prioritize reliability and redundancy, often featuring redundant servers, storage systems, and network architecture to minimize downtime and data loss.

Security: High-cost solutions include robust security features, such as encryption, authentication mechanisms, and secure access control, to protect sensitive video data from unauthorized access and cyber threats.

Customization and Integration: Organizations can often customize high-cost solutions to meet their specific needs, and they offer seamless integration with other IIoT technologies, providing a tailored and cohesive system.

Support and Maintenance: High-cost solutions typically include comprehensive support and maintenance packages, ensuring the system operates at peak performance and receives timely updates and troubleshooting assistance.

Use Cases:

Critical Infrastructure: High-cost solutions are essential for applications involving critical infrastructure, such as nuclear power plants, airports, and defense facilities, where system reliability, security, and performance are non-negotiable.

Large-Scale Manufacturing: Manufacturing operations with complex processes and stringent quality control requirements benefit from high-cost solutions to ensure production efficiency and product quality.

Real-time Decision-Making: Applications that require real-time decision-making, such as security and surveillance, rely on high-cost solutions for low latency and advanced analytics.

2. Low-Cost Solutions:

Overview: Low-Cost Solutions emphasize cost-effectiveness and affordability, prioritizing budget constraints while still providing basic video streaming capabilities. These solutions are characterized by their lower initial costs, making them accessible to a wider range of organizations, but they may have limitations in terms of features and performance.

Key Aspects:

Affordability: Low-cost solutions are budget-friendly, making them suitable for organizations with limited resources or cost constraints.

Basic Features: These solutions offer fundamental video streaming capabilities, including live video feeds and basic recording, without the advanced features and performance characteristics of high-cost alternatives.

Simplified Architecture: Low-cost solutions typically have simplified architectures, which can be easier to set up and manage, requiring less technical expertise.

Scalability Considerations: While not as scalable as high-cost solutions, some low-cost options may still provide limited scalability to accommodate modest growth.

Minimal Support and Maintenance: Support and maintenance packages for low-cost solutions may be less extensive, potentially requiring organizations to handle more management and troubleshooting tasks internally.

Koffka Khan, “A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT),” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

Use Cases:
Small Businesses: Small businesses with limited budgets can benefit from low-cost solutions for basic security and monitoring needs, such as retail stores or small manufacturing operations.
Entry-Level Deployments: Organizations looking to dip their toes into video streaming in the IIoT may start with low-cost solutions for pilot projects or proof-of-concept deployments.
Temporary Installations: Low-cost solutions are suitable for temporary or short-term video streaming needs, such as event monitoring or construction site surveillance.

In summary, the choice between High-Cost Solutions and Low-Cost Solutions within the VSIIoT Taxonomy's Cost and Budget category should be guided by the specific financial resources, operational requirements, and performance expectations of the industrial application. High-Cost Solutions offer advanced features, security, and reliability but require a higher initial investment. Low-Cost Solutions are budget-friendly and accessible but may have limitations in terms of features and scalability. The decision should align with the organization's budget constraints and the intended use and scale of the video streaming system.

This taxonomy illustrates the various facets of video streaming in IIoT, showcasing the diversity of applications, technologies, and considerations involved in implementing video solutions for industrial environments. Depending on specific use cases and requirements, organizations can tailor their video streaming systems to align with their goals and constraints.

IV. VSIIoT Component Comparisons

Let's compare the key components of the Video Streaming in Industrial IoT (VSIIoT) Taxonomy:
1. Network Architecture:
Edge Streaming: Processing and streaming video data at the edge of the network, closer to the data source.
Cloud Streaming: Sending video data to a central cloud server for processing and storage before streaming to end-users or devices.
2. Streaming Protocol:
Real-time Transport Protocol (RTP): A common protocol for streaming real-time multimedia data.
HTTP-based Streaming: Using HTTP-based protocols such as HTTP Live Streaming (HLS) or Dynamic Adaptive Streaming over HTTP (DASH) for video delivery.
3. Video Quality and Resolution:
Low-Resolution Streaming: Transmitting lower quality video to conserve bandwidth.
High-Resolution Streaming: Transmitting high-definition video for detailed monitoring.
4. Latency:
Low-Latency Streaming: Minimizing the delay between capturing and displaying video data.
High-Latency Streaming: Accepting some delay for improved video quality and reliability.
5. Camera Type:
Fixed Cameras: Stationary cameras capturing specific areas continuously.
Pan-Tilt-Zoom (PTZ) Cameras: Adjustable cameras for remote control and monitoring.
360-Degree Cameras: Cameras that capture panoramic views of an area.
6. Security and Authentication:
Secure Streaming: Employing encryption and authentication mechanisms to protect video data from unauthorized access.
Non-Secure Streaming: Transmitting video without advanced security measures.
7. Use Cases:
Surveillance and Security: Monitoring and securing critical infrastructure and assets.
Predictive Maintenance: Using video data for machine health analysis and fault prediction.
Process Monitoring: Monitoring industrial processes to optimize efficiency and quality.
Quality Control: Inspecting products for defects in manufacturing.
8. Integration with Other IIoT Technologies:
Sensor Integration: Combining video data with sensor data for more comprehensive insights.
Cloud Integration: Incorporating video streams into broader IIoT cloud-based platforms.
9. Data Storage:
Real-time Streaming: Discarding video data after real-time analysis without saving it.
Video Recording: Storing video data for historical analysis, compliance, or evidence.
10. Analytics and Machine Learning:
On-the-fly Analytics: Analyzing video data in real-time for immediate decision-making.
Post-processing Analytics: Applying machine learning and analytics to stored video data for insights and trends.
11. Scalability:
Scalable Streaming: Systems that can accommodate an increasing number of cameras and users.
Non-Scalable Streaming: Limited in terms of camera or user capacity.
12. Regulatory Compliance:
Compliance-Oriented Streaming: Meeting specific industry or regional regulations for video data.
13. User Access:
Remote Access: Allowing authorized users to view video feeds from anywhere.
Local Access: Restricting video streaming to a local network or physical proximity.
14. Cost and Budget:
High-Cost Solutions: Investing in advanced and robust video streaming systems.
Low-Cost Solutions: Opting for cost-effective video streaming solutions.

These components provide a comprehensive framework for categorizing and understanding the various aspects of video streaming in the context of Industrial IoT. Each component represents a critical decision point when designing, implementing, or evaluating video streaming systems for industrial applications, allowing organizations to tailor their solutions to their specific needs and requirements.

Koffka Khan, "A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT)," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

V. Uses Of VSIIoT Taxonomy

Here are use cases for each component of the Video Streaming in Industrial IoT (VSIIoT) Taxonomy:

1. Network Architecture:

Edge Streaming Use Case: In a smart factory, cameras at various production lines stream video data to edge devices for real-time quality control and process monitoring, reducing latency and enabling immediate responses.

Cloud Streaming Use Case: In a remote agricultural monitoring system, cameras on farmland send video data to a cloud server for processing and storage, allowing farmers to access and analyze data from anywhere.

2. Streaming Protocol:

RTP Use Case: In a real-time video conferencing system for remote technical support, RTP ensures low latency and high-quality video communication between field technicians and experts.

HTTP-based Streaming Use Case: In a smart city surveillance network, HTTP-based protocols like HLS are used to deliver video streams to central monitoring stations, ensuring compatibility with a wide range of devices.

3. Video Quality and Resolution:

Low-Resolution Streaming Use Case: In a traffic monitoring system, low-resolution video streams are used to reduce bandwidth usage while still providing sufficient visual information for traffic management.

High-Resolution Streaming Use Case: In a medical facility, high-resolution video feeds are critical for surgeons performing remote surgeries, enabling them to view fine details for precise procedures.

4. Latency:

Low-Latency Streaming Use Case: In an autonomous vehicle control system, low-latency video feeds are essential for real-time navigation and obstacle detection to ensure safe and efficient transportation.

High-Latency Streaming Use Case: In an industrial process monitoring application, higher latency is acceptable as long as the video quality is consistently high, allowing engineers to analyze processes and make informed decisions.

5. Camera Type:

Fixed Cameras Use Case: In a warehouse, fixed cameras are positioned to continuously monitor inventory levels and detect theft or unauthorized access.

PTZ Cameras Use Case: In a seaport security system, PTZ cameras are used to remotely monitor vessels, enabling security personnel to zoom in on suspicious activities.

360-Degree Cameras Use Case: In a retail store, 360-degree cameras provide a panoramic view to track customer behavior and optimize store layouts for increased sales.

6. Security and Authentication:

Secure Streaming Use Case: In a financial institution, secure streaming with encryption and authentication safeguards video data during remote meetings and transactions.

Non-Secure Streaming Use Case: In a research laboratory with open access to data, non-secure streaming may be acceptable for public demonstrations and educational purposes.

7. Use Cases:

Surveillance and Security Use Case: A critical infrastructure facility uses video streaming for real-time surveillance to detect and respond to unauthorized access or security breaches.

Predictive Maintenance Use Case: In a manufacturing plant, video data is analyzed to predict equipment failures and optimize maintenance schedules, reducing downtime and maintenance costs.

Process Monitoring Use Case: A chemical plant uses video streaming to monitor industrial processes, ensuring operations remain within specified parameters and quality standards.

Quality Control Use Case: An automotive manufacturing facility employs video streaming for real-time quality control, inspecting vehicles for defects in the production line to maintain high manufacturing standards.

8. Integration with Other IIoT Technologies:

Sensor Integration Use Case: In an agricultural IoT system, video data from surveillance cameras is integrated with environmental sensor data to monitor crop health and pest infestations.

Cloud Integration Use Case: In a smart city infrastructure management platform, video streams from traffic cameras are integrated into a broader cloud-based system for traffic analysis and optimization.

9. Data Storage:

Real-time Streaming Use Case: In a live sports broadcasting setup, video data is discarded after real-time transmission, as historical storage is unnecessary for sports events.

Video Recording Use Case: In a casino, video data is continuously recorded for compliance, security, and potential investigations into disputes or incidents.

10. Analytics and Machine Learning:

On-the-fly Analytics Use Case: In an e-commerce distribution center, on-the-fly analytics are used to track package sorting, detect anomalies, and optimize the flow of packages in real time.

Post-processing Analytics Use Case: In a retail store, post-processing analytics are applied to historical video data to identify customer behavior patterns and optimize store layout and product placement.

11. Scalability:

Scalable Streaming Use Case: An urban surveillance system continually expands to cover more areas and accommodate additional cameras and users as the city grows and demands increased security coverage.

Non-Scalable Streaming Use Case: A small-scale manufacturing operation maintains a fixed number of cameras and a limited user base for quality control and monitoring within a stable environment.

12. Regulatory Compliance:

Compliance-Oriented Streaming Use Case: In a healthcare facility, compliance-oriented streaming adheres to strict regulations like HIPAA to ensure patient data privacy and security during telemedicine consultations.

13. User Access:

Remote Access Use Case: In a global manufacturing company, authorized users can remotely access video feeds from multiple production facilities worldwide to monitor operations and quality control.

Koffka Khan, “A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT),” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

Local Access Use Case: In a secure research facility, access to video streams is restricted to users physically present within the facility, ensuring data privacy and protecting sensitive research.

14. Cost and Budget:

High-Cost Solutions Use Case: A large-scale oil refinery invests in high-cost video streaming solutions to ensure advanced security, reliability, and real-time monitoring of critical infrastructure.

Low-Cost Solutions Use Case: A small retail chain opts for low-cost video streaming solutions for basic security and surveillance, where budget constraints are a primary consideration.

These use cases illustrate how the components of the VSIIoT Taxonomy can be applied across various industrial applications, offering flexibility and adaptability to meet specific needs and requirements in the IIoT landscape.

VI. Discussion : The Significance of the Video Streaming in Industrial IoT (VSIIoT) Taxonomy

The Video Streaming in Industrial IoT (VSIIoT) Taxonomy is a structured framework that categorizes and defines the key components of video streaming in the context of the Industrial Internet of Things (IIoT). This taxonomy is of significant importance for several reasons:

Clarity and Understanding: The VSIIoT Taxonomy brings clarity to a complex and dynamic field. It categorizes and defines the various aspects of video streaming, helping stakeholders in the IIoT ecosystem understand the components and relationships involved. This clarity is essential for effective communication, collaboration, and decision-making.

Customization and Alignment: The taxonomy provides a framework for organizations to tailor their video streaming solutions to specific needs and objectives. By categorizing components like network architecture, streaming protocol, camera types, and more, it allows organizations to align their solutions with the unique requirements of their industrial applications.

Regulatory Compliance: In industries where regulatory compliance is crucial, such as healthcare, finance, and critical infrastructure, the Compliance-Oriented Streaming component of the taxonomy is particularly significant. It highlights the importance of adhering to industry or regional regulations for video data, reducing legal and reputational risks.

Security and Privacy: The taxonomy distinguishes between secure and non-secure streaming. In an era of increasing cyber threats and data breaches, organizations can use this classification to make informed choices about securing their video data. This is especially vital in applications where sensitive information is at risk.

Operational Efficiency: Understanding the components of the taxonomy allows organizations to make decisions that enhance operational efficiency. They can select the right level of video quality, latency, and scalability for their specific use cases, optimizing performance and cost-effectiveness.

Data-Driven Insights: Video data is a valuable source of insights in industrial applications. The VSIIoT Taxonomy encourages organizations to think about how they can apply analytics and machine learning to their video data, leading to data-driven decision-making and process improvements.

Cost Management: The Cost and Budget component of the taxonomy is crucial for organizations with budget constraints. It offers a clear distinction between high-cost and low-cost solutions, helping organizations make choices that align with their financial resources and needs.

Use Cases: The taxonomy's use cases provide real-world examples of how each component can be applied. These use cases illustrate the flexibility and adaptability of the taxonomy in diverse industrial applications, from manufacturing and security to healthcare and agriculture.

Motivation for the Taxonomy: The taxonomy's motivation underscores the real-world challenges and opportunities that organizations face in the IIoT landscape. It emphasizes the evolving nature of technology, regulatory requirements, and the need for informed decision-making.

In conclusion, the VSIIoT Taxonomy is a valuable tool for stakeholders in the IIoT ecosystem. It provides a structured framework that aids in decision-making, regulatory compliance, and the optimization of video streaming solutions for a wide range of industrial applications. As the IIoT continues to evolve, this taxonomy serves as a reference point for organizations seeking to harness the power of video streaming to enhance their operations and processes.

VII. Conclusion : The Role of the Video Streaming in Industrial IoT (VSIIoT) Taxonomy

The Video Streaming in Industrial IoT (VSIIoT) Taxonomy is a comprehensive and structured framework that categorizes the key components of video streaming within the context of the Industrial Internet of Things (IIoT). This taxonomy serves as a valuable reference for organizations, professionals, and stakeholders involved in the deployment, management, and evaluation of video streaming systems in industrial applications. The taxonomy's significance and implications can be summarized as follows:

Clarity and Understanding: The taxonomy brings clarity to the multifaceted field of video streaming in the IIoT. It defines and categorizes components, allowing for clear communication and an enhanced understanding of the various facets involved in video streaming.

Customization and Alignment: Organizations can utilize the taxonomy to tailor their video streaming solutions to specific industrial needs and objectives. This alignment ensures that the chosen components and configurations align with the unique requirements of the application.

Regulatory Compliance: In industries governed by stringent regulations and standards, the Compliance-Oriented Streaming component of the taxonomy highlights the importance of adhering to these rules, mitigating legal and reputational risks while maintaining data integrity and security.

Security and Privacy: The classification of secure and non-secure streaming underscores the significance of safeguarding video data in an era of escalating cyber threats. Organizations can make informed choices about securing their video data, particularly in applications where data privacy and confidentiality are critical.

Koffka Khan, “A Video Streaming in Industrial Internet of Things Taxonomy (VSIIoT),” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 5, pp. 148-164, 2023.

Operational Efficiency: The taxonomy empowers organizations to make decisions that optimize operational efficiency. By selecting the right levels of video quality, latency, and scalability, organizations can enhance performance while managing costs effectively.

Data-Driven Insights: The inclusion of analytics and machine learning components highlights the potential for deriving valuable insights from video data. By applying analytics and machine learning techniques, organizations can harness data-driven decision-making and process improvements.

Cost Management: The Cost and Budget component is of significant importance to organizations with budget constraints. It distinguishes between high-cost and low-cost solutions, enabling organizations to make choices that align with their financial resources and specific needs.

Use Cases: The taxonomy's use cases provide practical examples of how each component can be applied across a spectrum of industrial applications. These use cases illustrate the taxonomy's versatility and adaptability in real-world scenarios, from manufacturing and security to healthcare and agriculture.

In conclusion, the Video Streaming in Industrial IoT (VSIIoT) Taxonomy is a valuable tool that enhances the understanding, implementation, and management of video streaming solutions in the context of the IIoT. As the IIoT landscape continues to evolve, this taxonomy serves as a foundational reference, supporting organizations in their efforts to harness the power of video streaming to optimize industrial processes, enhance security, and drive innovation. The taxonomy's role extends beyond categorization; it is a guide and framework for the successful integration of video streaming in industrial applications, shaping a more efficient and secure future for the IIoT.

REFERENCES

[1] Akhtar, M.M., Rizvi, D.R., Ahad, M.A., Kanhere, S.S., Amjad, M. and Coviello, G., 2021. Efficient data communication using distributed ledger technology and iota-enabled internet of things for a future machine-to-machine economy. Sensors, 21(13), p.4354.

[2] Baars, H., Tank, A., Weber, P., Kemper, H.G., Lasi, H. and Pedell, B., 2021. Cooperative approaches to data sharing and analysis for industrial internet of things ecosystems. Applied Sciences, 11(16), p.7547.

[3] Kebande, V.R., 2022. Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0. Forensic Science International: Reports, 5, p.100257.

[4] Khan, J., Khan, G.A., Li, J.P., AlAjmi, M.F., Haq, A.U., Khan, S., Ahmad, N., Parveen, S., Shahid, M., Ahmad, S. and Raji, M., 2022. Secure smart healthcare monitoring in industrial internet of things (iiot) ecosystem with cosine function hybrid chaotic map encryption. Scientific Programming, 2022.

[5] Khan, K. and Goodridge, W., 2017. Server-based and network-assisted solutions for adaptive video streaming. International Journal of Advanced Networking and Applications, 9(3), pp.3432-3442.

[6] Khan, K. and Goodridge, W., 2018. Future DASH applications: A survey. International Journal of Advanced Networking and Applications, 10(2), pp.3758-3764.

[7] Khan, K. and Goodridge, W., 2018. QoE in DASH. International Journal of Advanced Networking and Applications, 9(4), pp.3515-3522.

[8] Khan, K. and Goodridge, W., 2020. QoE evaluation of dynamic adaptive streaming over HTTP (DASH) with promising transport layer protocols: Transport layer protocol performance over HTTP/2 DASH. CCF Transactions on Networking, 3(3-4), pp.245-260.

[9] Khan, K. and Goodridge, W., Markov Decision Processes for bitrate harmony in adaptive video streaming. In 2017 Future Technologies Conference (FTC), Vancouver, Canada, unpublished.

[10] Koffka, K. and Wayne, G., 2018. A DASH Survey: the ON-OFF Traffic Problem and Contemporary Solutions. Computer Sciences and Telecommunications, (1), pp.3-20.

[11] Madakam, S. and Uchiya, T., 2019. Industrial internet of things (IIoT): principles, processes and protocols. The Internet of Things in the Industrial Sector: Security and Device Connectivity, Smart Environments, and Industry 4.0, pp.35-53.

[12] Magaia, N., Fonseca, R., Muhammad, K., Segundo, A.H.F.N., Neto, A.V.L. and de Albuquerque, V.H.C., 2020. Industrial internet-of-things security enhanced with deep learning approaches for smart cities. IEEE Internet of Things Journal, 8(8), pp.6393-6405.

[13] Mahmood, A., Beltramelli, L., Abedin, S.F., Zeb, S., Mowla, N.I., Hassan, S.A., Sisinni, E. and Gidlund, M., 2021. Industrial IoT in 5G-and-beyond networks: Vision, architecture, and design trends. IEEE Transactions on Industrial Informatics, 18(6), pp.4122-4137.

[14] Munirathinam, S., 2020. Industry 4.0: Industrial internet of things (IIOT). In Advances in computers (Vol. 117, No. 1, pp. 129-164). Elsevier.

[15] Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M. and Wu, D.O., 2020. Edge computing in industrial internet of things: Architecture, advances and challenges. IEEE Communications Surveys & Tutorials, 22(4), pp.2462-2488.

[16] Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M. and Wu, D.O., 2020. Edge computing in industrial internet of things: Architecture, advances and challenges. IEEE Communications Surveys & Tutorials, 22(4), pp.2462-2488.

[17] Sari, A., Lekidis, A. and Butun, I., 2020. Industrial networks and IIoT: Now and future trends. Industrial IoT: Challenges, Design Principles, Applications, and Security, pp.3-55.

[18] Sari, A., Lekidis, A. and Butun, I., 2020. Industrial networks and IIoT: Now and future trends. Industrial IoT: Challenges, Design Principles, Applications, and Security, pp.3-55.

[19] Vijayaraghavan, V. and Rian Leevinson, J., 2019. Internet of things applications and use cases in the era of industry 4.0. The Internet of Things in the Industrial Sector: Security and Device Connectivity, Smart Environments, and Industry 4.0, pp.279-298.

[20] Zhang, P., Wu, Y. and Zhu, H., 2020. Open ecosystem for future industrial Internet of things (IIoT): architecture and application. CSEE Journal of Power and Energy Systems, 6(1), pp.1-11.

[21] Zheng, P., Xu, X. and Wang, L., 2023. Editorial notes: Industrial Internet-of-Things (IIoT)-enabled digital servitisation. International Journal of Production Research, 61(12), pp.3844-3848.