Research on an Industrial Internet Data Encryption Architecture Based on Quantum Key Distribution

Peng Deng

{2124667563@qq.com}

Wuhan University of Science and Technology, 947 Heping Avenue, Qingshan District, Wuhan City, Hubei Province, China

Abstract. The industrial internet represents critical infrastructure that integrates modern information and communication technologies with industrial systems, driving the fourth industrial revolution. It enables industries to achieve digitalization, networking, and intelligent development, thereby enhancing operational efficiency, reducing costs, and promoting sustainable manufacturing. However, with the rapid adoption of technologies such as 5G, big data, and artificial intelligence, the industrial internet faces increasingly complex security challenges, particularly in data transmission. Traditional encryption methods often struggle to meet the stringent security and performance demands of industrial environments. This paper proposes a novel data encryption architecture for the industrial internet that combines quantum key distribution (QKD), using the BB84 protocol, with active wavelength division multiplexing (WDM). This hybrid approach ensures robust security while optimizing data transmission over long distances. Two encryption schemes are introduced: one for high-volume data transfers and another for cost-sensitive, lower-volume applications. Simulation results demonstrate that increasing the average number of photons per pulse enhances the key generation rate (KGR), significantly improving key establishment speed and data signal utilization in industrial applications. Additionally, optimizing dark counts reduces the quantum bit error rate (QBER), further enhancing system reliability. The architecture's flexibility allows it to be adapted to various industrial use cases, ranging from large-scale data transfers to low-cost secure communications. In conclusion, the proposed solutions effectively enhance data transmission efficiency while maintaining high levels of security, positioning the industrial internet for further growth and innovation.

Keywords: industrial internet, quantum key distribution, wavelength division multiplexing.

1 Introduction

The industrial internet is a new type of infrastructure, application model, and industrial ecosystem that integrates modern information and communication technology with the industrial economy. It provides a pathway for the digitalization, networking, and intelligent development of industry, serving as a cornerstone of the fourth industrial revolution [1]. The functional architecture of the industrial internet comprises three major systems: network, platform, and security [2].

The industrial internet's importance can be understood in two main aspects. First, it provides essential support for building a robust manufacturing sector, promoting the transformation and

CONF-MLA 2024, November 21, Adana, Turkey

DOI 10.4108/eai.21-11-2024.2354643

upgrading of traditional industries. It enables the optimization of resource allocation across a broader range of production and service resources with greater efficiency and precision. This optimization achieves quality improvement, cost reduction, efficiency gains, and advancements in sustainable and secure development, thus supporting high-end, intelligent, and green manufacturing. Consequently, the industrial internet significantly enhances the quality and efficiency of industrial economic development [3]. Accelerating the development of emerging industries strengthens the industrial internet, driving end-to-end digitalization in industrial production towards full integration. This shift accelerates profound transformations in innovation methods, production models, organizational structures, and business paradigms [4]. Second, advancing the evolution and upgrading of the industrial internet enhances the supporting capabilities of network infrastructure [5]. The industrial internet's high permeability allows deep integration across multiple industries, facilitating the scientific transition of network applications from virtual to physical domains, from daily life to industrial production, and significantly expanding the scope of the digital economy [6].

However, security threats to the industrial internet remain. Several countries have accelerated the development of relevant standards, issuing guidelines such as the General Requirements for Industrial Internet Security Protection, the Industrial Internet Platform Security Protection Requirements, and the Industrial Internet Comprehensive Standardization System Construction Guide. These documents have contributed to a preliminary security standard system that includes equipment security, control security, network security, data security, application security, platform security, and security management [7]. Additionally, the market for protective products has expanded, spurring growth in the security training service market and further optimizing the industrial structure. In response to compliance requirements, industrial enterprises must continue to enhance their safety protection systems, strengthen security responsibilities, increase security investments, and implement comprehensive security planning and infrastructure [8]. There is also a critical focus on ensuring the autonomy and controllability of information security products, with a national priority on locally produced security solutions to strengthen national security through independent innovation [9]. Ultimately, both IT and OT security demands must be addressed to improve the overall security framework for industrial enterprises. A primary objective in this context is to ensure production continuity and reliability. Traditional IT security solutions, often characterized by high network latency or cost, are generally unsuited for OT networks. Therefore, it is essential to develop technical solutions that balance security risks with business impact, tailored specifically to the characteristics of OT networks [10].

2 Literature Review

The industrial internet has made significant strides in recent years. Firstly, the scale of China's industrial internet industry has surpassed 1.2 trillion RMB, supported by the integration of next-generation information technologies such as the industrial Internet of Things (IoT), big data analytics, cloud computing, and artificial intelligence. These advancements address evolving market demands and challenges, while simultaneously introducing more uncontrollable risks and security issues [11]. The industrial internet primarily manages data related to entities like sensors and production equipment, focusing on production process monitoring, production operation optimization, anomaly detection, and network security [12]. Future applications of the

industrial internet may include traffic data infrastructure, model interpretability and robustness, adversarial machine learning, and its defenses [13]. Additionally, the construction of a 5G (the fifth generation mobile communication technology) converged network for industrial applications and the development of internal and external networks for industrial internet enterprises present technical challenges. The integration of 5G technology and the industrial internet faces three key technological hurdles: real-time traffic identification for 5G and intelligent manufacturing networks, dynamic service migration within these networks, and the convergence and fusion of heterogeneous data [14].

This paper addresses a critical issue for the industrial internet: as technologies like 5G, cloud computing, and IoT advance, they become increasingly susceptible to security risks, particularly data breaches and cyberattacks. The complexity of industrial data networks, coupled with the need for real-time processing and low-latency communication, necessitates an encryption solution that is both highly secure and efficient without adding substantial overhead to network infrastructure. To address this challenge, this paper proposes a data encryption transmission architecture for the industrial internet based on a hybrid approach that combines quantum key distribution (QKD) with wavelength division multiplexing (WDM) technology.[15] This approach effectively overcomes the challenge of secure key exchange over long distances, a major bottleneck in current industrial network systems. In conclusion, this paper offers a practical solution to the critical issue of secure, scalable data transmission within the industrial internet. By implementing a quantum-enhanced encryption framework, this architecture ensures the confidentiality and integrity of sensitive industrial data, positioning the industrial internet for future growth in a highly secure and efficient manner. This solution paves the way for safer smart factories, industrial automation, and critical infrastructure systems, while maintaining the flexibility to adapt to emerging technologies.

3 Quantum Key Distribution

The BB84(a protocol based on quantum key distribution) protocol, proposed in 1984, is the earliest quantum key distribution (QKD) protocol and remains the most mature and widely used QKD protocol to date. Its security has been rigorously demonstrated. The original protocol uses a single photon as the information carrier, encoding information through the four polarization states of light. These states are divided into two groups of conjugate bases, with each group containing two orthogonal polarization states. The two bases selected by the BB84 protocol are the horizontal-vertical and diagonal bases. Since these bases are in non-orthogonal spaces, every vector in one basis has an equal projection onto each vector in the other basis. As a result, if the sender and receiver use different bases, the detection result is random with equal probability. If the same bases are used, detection will yield a definitive result or indicate photon non-detection.

The key distribution process of BB84 is as follows, with the sender referred to as Alice and the receiver as Bob:

Step 1: Establish a convention for information encoding, including the use of orthogonal conjugate bases and the correspondence between each quantum state and binary information. Using the horizontal-vertical and diagonal bases as an example, 0° and 45° polarizations correspond to binary bit 0, while 90° and 135° polarizations correspond to binary bit 1.

Step 2: Alice prepares a single photon as the carrier of quantum information.

Step 3: Alice generates a random sequence and randomly selects one of the two bases. According to the random sequence, the photon is modulated into the corresponding quantum state. For example, a polarization beam splitter is used to select the horizontal-vertical bases, and adding a quarter-wave plate allows selection of the 45°and 135° bases.

Step 4: Upon arrival at Bob's end, he randomly selects either the horizontal-vertical or diagonal bases for measurement. The polarization beam splitter and quarter-wave plate complete the photon measurement process. Since photons may attenuate in transit, not every photon sent by Alice will be detected by Bob. Bob records the positions of detected photons as valid photons, while others are presumed lost in the quantum circuit. Alice and Bob’s subsequent steps are applied only to valid photons.

Step 5: Bob announces the measurement basis he used. If Alice used the same basis for modulation, she informs Bob of a successful match, and both retain the polarization states for this transmission.

Step 6: Based on the retained polarization states and the pre-established relationship between polarization states and binary bits ("0" and "1"), both parties generate their respective key sequences.

During protocol execution, the basis used for measurement is publicly shared over a classical channel, making it vulnerable to eavesdropping by a third party, commonly referred to as Eve. However, Eve, like Bob, can only randomly select measurement bases and has only a 25% chance of obtaining the correct information. The remaining 25% will introduce error codes, which Alice and Bob can detect when they compare results. Although Eve may attempt more sophisticated methods, these are constrained by the fundamental properties of quantum mechanics.

4 . Industrial Internet Data Encryption Transmission Architecture

There are several options for 5G fronthaul solutions, with the most commonly used being direct fiber connection, passive wavelength division multiplexing (WDM), and active WDM.

First, in the direct fiber connection scheme, the active antenna unit (AAU) and the distributed unit (DU) are directly connected by optical fiber. Both AAU and DU are equipped with 25Gbps white light modules, supporting transmission distances of up to 10 km. To conserve fiber resources, the industry has developed a 25Gbps bidirectional solution with integrated WDM functionality. In this configuration, bidirectional data signals between AAU and DU are transmitted within the same optical fiber using different wavelengths, which reduces fiber resource usage by half. However, even with this technology, a DU that connects to 10–20 AAUs still requires a substantial amount of fiber, placing additional demands on fiber management at the DU. Thus, fiber resources and management represent key limitations for this solution.

Second, in the passive WDM scheme, an end-to-end, fully passive, low-cost WDM transmission is implemented without the need for relay amplification or dispersion compensation. The AAU utilizes color light modules, connecting to a passive combiner or splitter through branch optical cables. At the DU (central office), wavelength multiplexing or demultiplexing is achieved using

a passive combiner/splitter, establishing a one-to-one correspondence between each AAU and the central office using specific color wavelengths. Despite its simplicity in deployment, this scheme has drawbacks, such as a lack of fault management and maintenance challenges. Additionally, the number of wavelength channels in a passive dense wavelength division multiplexing (DWDM) system is limited, which complicates network management during expansion.

Third, in the active WDM solution, outdoor active WDM equipment is used to perform electrical or optical layer multiplexing at both remote and central stations. This approach reduces the number of endpoint fibers required. It supports various topologies—such as ring, loop, chain, and star configurations—and provides telecom-grade manageability. The active DWDM system also supports a greater number of wavelength channels, resulting in increased bandwidth and better fiber utilization. However, this solution comes at a higher cost and is constrained by factors like base station power supply conditions.

Based on the analysis of these different schemes, although active WDM is more costly than direct fiber connections, it allows for longer-distance transmission. Compared to passive WDM, active DWDM systems offer greater transmission distances and easier management. Channels can be adjusted online without shutting down the system, and network expansion is more straightforward. In summary, active WDM has distinct advantages over other solutions. Building on these findings, we propose, for the first time, an industrial internet signal encryption method that integrates active WDM with quantum signals based on the BB84-QKD protocol.

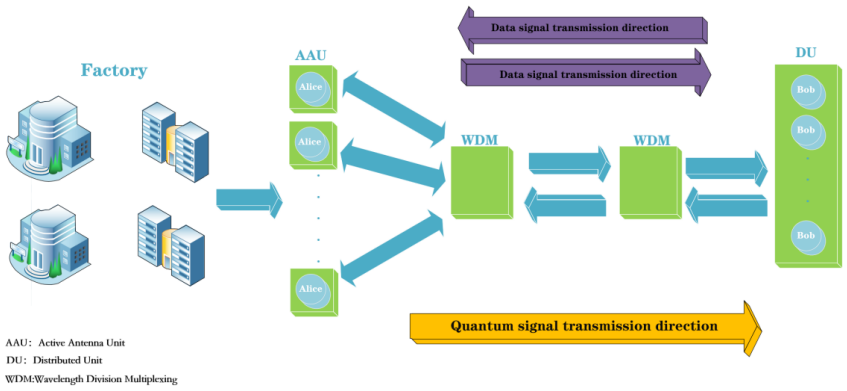

Fig. 1. Industrial Internet Efficient Data Encryption Transmission Architecture

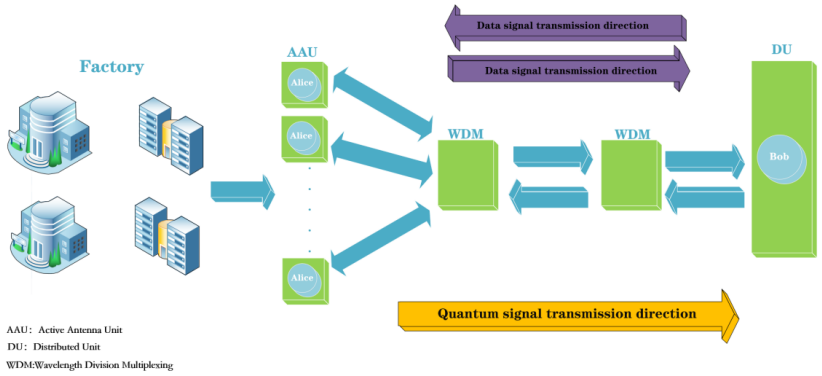

Fig. 2. Industrial Internet Data Encryption Transmission Architecture-+

To address these needs, we propose two solutions: the Industrial Internet Efficient Data Encryption Transmission Architecture and the Industrial Internet Data Encryption Transmission Architecture, as illustrated in Figures 1 and 2. In the communication process, signals are primarily categorized as either data signals or quantum signals. Data signals refer to the content transmitted between the active antenna unit (AAU) and the distributed unit (DU). For example, when data flows from the AAU to the DU, the process begins with the factory transmitting data to the AAU through email or cloud storage links. The AAU then sends the data signal to the Wavelength Division Multiplexer (WDM). Subsequently, the WDM transmits the data through optical fibers to the corresponding WDM, which ultimately forwards the data signal to the DU for temporary storage. Data transmission from the DU to the AAU follows the same process in reverse.

Quantum signals refer to the measurement bases used by Alice and Bob in the BB84 protocol. Initially, Alice transmits the quantum signal to the WDM associated with the AAU, which then sends it via optical fibers to the WDM connected to the DU. Finally, the signal reaches Bob, located within the DU, where base matching occurs. If the bases match, the data can be read successfully; if they do not, the data cannot be retrieved.

Next, we discuss the two solutions individually. The Industrial Internet Efficient Data Encryption Transmission Architecture utilizes a higher number of Bobs and a lower number of Alices, effectively enhancing the measurement base matching rate while maintaining high security. This scheme is typically applied in scenarios requiring substantial data transfer or high transmission rates, such as in large-scale factory data transfers, online gaming, cloud computing, the Internet of Things (IoT), scientific research, and medical imaging. However, the extensive use of Bobs results in significantly higher costs.

In contrast, the Industrial Internet Data Encryption Transmission Architecture employs more Alices and fewer Bobs, making it suitable for scenarios with lower data transfer volumes or less stringent transmission rate requirements. This configuration effectively reduces costs and is generally applied in contexts such as email transmission and simple web browsing. The primary

advantage of this architecture lies in its ability to achieve secure data transmission at a lower cost, offering a favorable cost-performance ratio.

In summary, our proposed framework ensures the secure transmission of information, preventing data leakage and meeting encryption requirements for information communication. Additionally, this framework can be applied within industrial internet and military sectors to guarantee information security and reliability. The framework is also highly portable, as simply installing Alice and Bob externally enables encryption functionality. Finally, continuous updates to the framework will improve security performance without requiring complex modifications to the finished product, demonstrating excellent scalability and adaptability.

5 . Performance Analysis of QKD

Based on the previous analysis, we conducted simulations to evaluate the performance of quantum key distribution (QKD) in terms of efficiency, the average number of photons per pulse, and the dark count rate per unit pulse. These simulations examine the impact of these variables on the quantum bit error rate (QBER) and the key generation rate (KGR), as illustrated in Figures 3, 4, and 5.

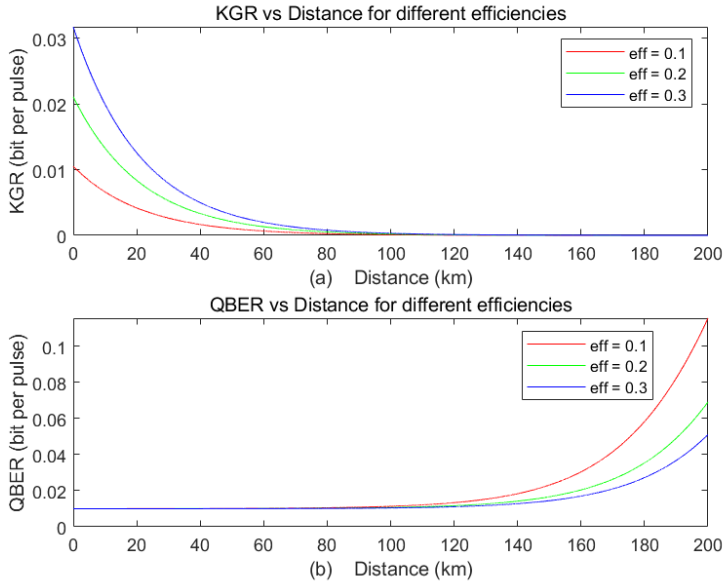

Fig. 3. The impact on QBER and KGR under different efficiency data. (KGR: key generation rate; QBER: quantum bit error rate)

In relation to Figure 3, we observe the following trends: Firstly, the key generation rate (KGR) exhibits an overall decreasing trend as distance increases, approaching zero beyond 80 km. Additionally, for any given distance, a higher efficiency (eff) value results in a faster KGR. Secondly, the quantum bit error rate (QBER) shows an overall increasing trend with distance, with a marked rise only when the distance exceeds 100 km. Moreover, for a given distance, a

lower efficiency value is associated with a higher QBER. When employing the Industrial Internet Efficient Data Encryption Transmission architecture to encrypt signals, we observe a significant improvement in the KGR, which greatly benefits data signal transmission. Additionally, the QBER is substantially reduced, enhancing the success rate of key matching and increasing the overall efficiency of signal transmission.

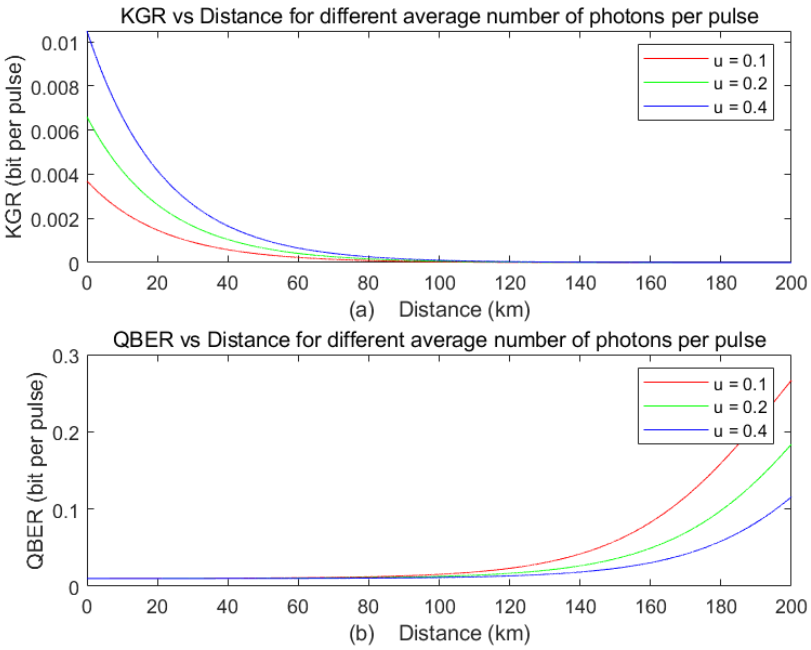

Fig. 4. The impact on QBER and KGR under different average number of photons per pulse. (u: average number of photons per pulse)

In relation to Figure 4, we observe the following trends: Firstly, a larger average number of photons per pulse (u) correlates with a slightly lower key generation rate (KGR). However, the differences in KGR between various u values are relatively minor, and this discrepancy further diminishes as the transmission distance increases. Secondly, a smaller u value is associated with a higher quantum bit error rate (QBER), and the disparity in QBER between different u values widens with increasing distance. In simulations, increasing the average number of photons per pulse during transmission from the active antenna unit (AAU) to the distributed unit (DU) significantly enhances the KGR, enabling faster key establishment. This improvement also boosts data signal utilization within the Industrial Internet, aligning more effectively with industrial requirements.

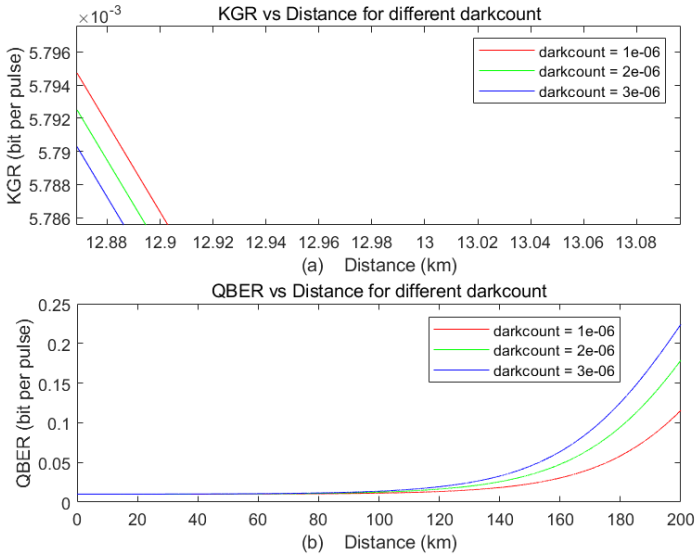

Fig. 5. The impact on QBER and KGR under different e unit pulse value of the darkcount (darkcount: the unit pulse value of the darkcount)

In relation to Figure 5, we observe the following trends: Altering the unit pulse value of the dark count has minimal impact on the key generation rate (KGR). However, for any given distance, a moderate increase in the dark count per unit pulse leads to a reduction in the quantum bit error rate (QBER), with the extent of this reduction becoming more pronounced as distance increases. Within the quantum 5G architecture, we find that incrementally increasing the dark count per unit pulse reduces the error rate in key generation. This outcome is particularly beneficial for our industrial internet efficient data encryption transmission architecture, as it enhances the overall system reliability and performance.

6 Conclusions

This paper presents an innovative industrial internet encryption architecture that combines quantum key distribution (QKD) with active wavelength division multiplexing (WDM), thereby enhancing both the security and efficiency of industrial data transmission. The core innovation of this architecture lies in the seamless integration of the BB84-QKD protocol, a well-established quantum cryptographic standard, with modern 5G networks. This approach offers a secure communication method capable of meeting the growing demand for secure data exchange in industrial environments. Simulation results demonstrate that increasing the average number of photons per pulse enhances the key generation rate (KGR), directly improving the speed of secure key establishment. Additionally, system performance is further optimized by reducing the quantum bit error rate (QBER), leading to more reliable and efficient communication. In terms of application potential, the proposed architecture is highly adaptable to a variety of industrial scenarios, making it a robust solution for secure data transmission in industrial automation, cloud-based operations, and industrial IoT systems. For high-data-

volume environments, such as smart manufacturing or real-time industrial monitoring, the industrial internet efficient data encryption transmission architecture provides superior security without compromising transmission speed, ensuring that large-scale data exchanges remain both secure and efficient. For lower data-intensive applications, such as email communications or remote monitoring, the industrial internet data encryption transmission architecture offers a cost-effective solution that balances security with resource efficiency. Overall, this architecture not only addresses current security challenges in the industrial internet but also lays a foundation for future applications in areas such as autonomous systems, 5G-based manufacturing, and critical infrastructure protection. It supports the secure and scalable growth of the industrial sector, positioning it for continued advancement.

References

[1] Zhang, Y., & Wang, J. "Industrial Internet of Things: A Review." IEEE Internet of Things Journal, 8(2), 1072-1091, Tue, 23 Nov 2021.

[2] Li, S., et al. "Industrial Internet and Smart Manufacturing: A Comprehensive Review." International Journal of Advanced Manufacturing Technology, 109(9-12), 2817-2832, Thu, 22 Feb 2024

[3] Gupta, S., & Singh, R. "Cybersecurity in Industrial Internet of Things: A Review." Computers & Security, 113, 102543, February 2022

[4] Ding, Y., & Zhang, J. "5G Networks and Industrial Internet of Things: A Review." IEEE Access, 11, 5472-5485, Thu, 22 Feb 2024.

[5] Xu, K., et al. "Quantum Key Distribution for the Industrial Internet of Things." IEEE Transactions on Information Theory, 67(8), 5527-5540, 28 Aug 2024.

[6] Chen, J., et al. "Data Security and Privacy in Industrial IoT: A Survey." IEEE Internet of Things Journal, 9(7), 5775-5790,04 August 2021.

[7] Zhao, X., et al. "Integrating 5G and Edge Computing for the Industrial Internet." Future Generation Computer Systems, 136, 165-179,23 June 2020 .

[8] Qiu, J., et al. "Challenges and Opportunities in Securing the Industrial Internet." Journal of Network and Computer Applications, 170, 102779, September 2020.

[9] Wang, T., & Zhang, Q. "The Role of AI in Cybersecurity for Industrial IoT." Artificial Intelligence Review, 55(3), 2173-2195, April 2024.

[10] Liu, H., et al. "Big Data and the Industrial Internet: A Survey." IEEE Transactions on Industrial Informatics, 17(5), 3422-3433, November 2014.

[11] Fan, J., et al. "Edge Computing for the Industrial Internet of Things: A Survey." IEEE Communications Surveys & Tutorials, 22(4), 2674-2702, November 2017.

[12] Zhang, Y., et al. "Hybrid Encryption Techniques for Industrial Internet Security." Journal of Information Security and Applications, 70, 103141, June 09, 2024.

[13] Wang, Y., et al. "A Survey on Blockchain for Industrial IoT." IEEE Internet of Things Journal, 9(3), 2213-2236, January 2019.

[14] Khan, R., et al. "Emerging Security Challenges in the Industrial Internet of Things: A Comprehensive Review." Journal of Network and Computer Applications, 189, 103138, August 2021.

[15] Cheng, L., & Lu, Y. "Future Directions of Cybersecurity for Industrial Internet: A Review." Computers & Security, 118, 102778, 12 Oct 2024.