Navigating the Security Landscape of the Industrial Internet of Things in Industry 4.0: Frameworks, Issues and Solutions

1st Xuan Tuan Minh Nguyen
Dept. of Computer Science
Swinburne University of Technology
Hawthorn, VIC, Australia
103819212@student.swin.edu.au

Abstract—**Nowadays, the Industrial Internet of Things (IIoT) is considered one of the major components that contributes to the significant growth of Industry 4.0. Although it has introduced multiple benefits, a number of vulnerabilities regarding security have been exposed, and concerns have been raised due to its internal characteristics and the application environment. This report is written in order to demonstrate a comprehensive analysis of the security challenges that are exposed in the IIoT. It focuses on investigating the current frameworks and protocols, the current unsolved issues, and proposed solutions to these challenges. We will focus on highlighting the contributions towards protecting IIoT systems by some of the protocols that are commonly used in Industry 4.0, such as MQTT, DDS, and CoAP, as well as wide spreading frameworks like the NIST Framework and IEC 62443. While highlighting the contributions of the proposed protocols and frameworks, this research will discuss the remaining significant issues, specifically scalability, heterogeneity, and secure real-time monitoring and transmitting / receiving data, but also propose possible solutions that provide a deep perspective on the future of IIoT security, such as Unified Security Frameworks, Lightweight Cryptographic Solutions, Secure Lifecycle Management and Fog and Edge Computing. This report highlights the ever-changing IIoT security landscape, underscoring the importance of continuing research and development in this field.**

Keywords—Industrial Internet of Things (IIoT), IIoT Security, Message Queueing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Data Distribution Service (DDE), National Institute of Standards and Technology Framework (NIST), International Electrotechnical Commission's 62443 (IEC 62443), Scalability and Heterogeneity, Real-time Security Monitoring and Response, Unified Security Frameworks, Lightweight Cryptographic Solutions, Secure Lifecycle Management, Fog and Edge Computing, Industry 4.0

I. Introduction

In the revolution of Industry 4.0, The Industrial Internet of Things (IIoT) is an essential component that significantly helps transform formal industries by integrating physical machines with digital systems, allowing for fully empowering the capabilities of the network and utilising large-scale data analytics. While this paradigm shift introduces myriad benefits, it also proposes more modern and complex security issues that need to be immediately considered [1] [2].

In Industry 4.0, IIoT is well known by its operating condition as hazardous and dangerous, which it usually places in hazardous environments and controls dangerous system with strict timing requirements. With these characteristics, IIoT needs to consider following a unique set of security protocols and frameworks. Moreover, due to their scalability and distribution nature, IIoT networks also bring up an array of vulnerabilities that could be easily exploited by anyone to initialise an attack. [10]

This report dives into the presented IIoT security vulnerabilities, specifying on the developed security frameworks and protocols to defend against those issues, the challenges these frameworks and protocols aim to resolve, and the unseen security issues. Moreover, this report also analyses considerable solutions to navigate the landscape of unresolved issues and increase the security of IIoT.

This report starts by introducing a specific definition for each proposed framework and protocol that is currently being widely used, such as MQTT, DDS, and CoAP, as well as the extensive IEC 62443 standard and the famous Cybersecurity Framework NIST [11] [12] [13] [14] [15]. With a specific evaluation of these tools, it also uncovers the detailed issues regarding security and optimised data transmissions to assess the risk and system design that these frameworks / tools were created to solve.

Although these protocols and frameworks are robust, several major issues remain unanswered, mostly regarding scalability, heterogeneity, and monitoring and responding securely in real-time [16] [17]. This research aims to investigate these unanswered issues, their impacts on the security of IIoT, and solutions that could potentially mitigate those problems. These solutions include top-notch frameworks and strategies, such as Unified Security Frameworks, Lightweight Cryptographic Solutions, Secure Lifecycle management, and Fog and Edge Computing [3] [4] [5] [6] [7] [8] [9].

To address these statements, this research pivots a thorough and comprehensive inspection of IIoT security, adding to the ongoing conferences in academia and industry. With the complex and growing security concerns in IIoT, continuous research and development are crucial to protecting this vital topic of Industry 4.0

II. Frameworks and Protocols

The complex security demands of IIoT require the design and implementation of effective security frameworks and protocols. Multiple different frameworks and protocols have been introduced and are still in use today to ensure a secure connection, reliable operations, and data integrity within IIoT systems.

A. *Message Queueing Telemetry Transport (MQTT)*

The Message Queueing Telemetry Transport (MQTT) protocol is well-known as one of the most commonly used protocols in the market. MQTT, designed for lightweight information transfer, is broadly applied in IIoT and Industry 4.0 due to its performance in handling unreliable networks, making it suited for remote control applications in any industry. However, due to its lack of security capabilities, the use of a secure transport layer on top, for example, encryption with TLS/SSL protocols, is essential. [11]

B. *Constrained Application Protocol (CoAP)*

One brilliant IIoT protocol created for high resource-constraints is the Constrained Application Protocol (CoAP). CoAP is known due to its operability in both request-response and publish-subscribe modes without high consumption of resources, making it suitable for multiple different cases. Moreover, CoAP also built in security protections by empowering the Datagram Transport Layer Security protocols (DTLS) [12].

C. *Data Distribution Service (DDS)*

On the other hand, Data Distribution Service (DDS), which is used on real-time applications, focuses on providing fine-grained and data-centric security controls. In addition, due to its mechanism allowing secure data in both transit and rest modes, DDS is also known for its protection and reliability in real-time industry, where timely access is essential [13].

D. *National Institute of Standards and Technology (NIST)*

Regarding the Cybersecurity frameworks, the National Institute of Standards and Technology's Cybersecurity Frameworks, or in short, NIST Cybersecurity Frameworks, offer dynamic and customisable solutions for managing cybersecurity concerns in IIoT. It comprises five core categories—Identify, Protect, Detect, Respond, and Recover—that encompass the majority of aspects of cybersecurity, from exploring threats to mitigation and recovery [14].

E. *International Electrotechnical Commission's (IEC) 62443*

Identically, the International Electrotechnical Commission's 62443 standard (IEC 62443) provides detailed guidelines for protecting Industrial Control Systems (ICS). From designing a system to deployment and maintenance, including risk assessment, architecture design and secure development, the IEC 62443 standard covers most aspects from the security list of IEC 62443 [15].

III. The Aim of Current Frameworks and Protocols

The discussed protocols and frameworks in the context of IIoT were designed to navigate specific issues arising due to the characteristics and constraints of the IIoT landscape. These issues include ensuring reliable and secure data transmission, leveraging the integrity of the system, device authentication, protecting privacy, and dealing with resource-constrained devices.

A. *Unstable Networks*

The Message Queueing Telemetry Transport (MQTT) Protocol has been purposely created in order to operate on an unstable network environment where the network could be high-latency and sometimes unreliable. Its public-subscribe model enables for distributing packages efficiently, reducing the dependence for network bandwidth and latency. Due to its client and broker architecture, it reduces the need for continuous connection, thus increasing the overall performance in challenging network conditions. Moreover, its three-level Quality of Service (QOS) mechanism guarantees reliable message delivery in a hazardous network environment.

B. *Resource-Constrained Devices and Networks*

In order to provide a lightweight alternative to HTTP protocols, the Constrained Application Protocol (CoAP) was created to tackle resource-constrained devices and networks. CoAP engages with modern REST architecture, providing simple methods to interact with resources, such as GET, POST, PUT and DELETE, which can be identified by URIs and Headers. In addition, with the integration of Datagram Transport Layer Security (DTLS), CoAP ensures a safe connection, guards the integrity and confidentiality of data, and provides endpoint authentication.

C. *Securing real-time data transmission*

By prioritising data-centric and fine-grained security configurations, Data Distribution Service (DDS), which is crafted specifically for real-time solutions, is able to provide data-level access control, guarding authorised personnel from accessing specific resources. This is the pinnacle for any industry that requires permissions to access certain resources. Moreover, for DDS, data is encrypted when transmitted, ensuring the integrity and confidentiality of the data, as the data could not be decrypted once it got hijacked.

D. *ICS Security*

The IEC 62443 framework adopts a lifecycle view of Industrial Control Systems (ICS), providing guidelines from the design to the maintenance procedure. Which includes defining system requirements, system design, implementation, installation, operation, maintenance and decommissioning. The core model of this standard, which is a defence-in-depth model, offers multiple layers of security. This comprehensive framework ensures the elimination of any weaknesses in areas that do not compromise the entire system.

E. *Cybersecurity Management*

Aiming to provide a high-level strategy for managing cybersecurity issues, the NIST Framework offers comprehensive attention to cybersecurity vulnerabilities across every level of an organisation, thus ensuring that all users are aware of the dangers of the risks and actively involved in risk management. The framework is divided into five core procedures: Identify, Protect, Detect, Respond and Recover. These functions provide a detailed classification of cybersecurity outputs and organise the critical risks regarding cybersecurity attacks. Moreover, the proposed procedures also help in expressing cybersecurity issues by organising information, enabling dynamic risk management solutions, addressing threats, and improving through lessons learned from the past.

IV. Unresolved Issues

Although considerable progress has been made by the proposed security frameworks and protocols in the context of securing the IIoT, several concerns remain unaddressed. These concerns could be grouped into two major categories:

A. Scalability and Heterogeneity [16] [17]

In the context of IIoT, it consists of a wide range of devices, networks, protocols, and frameworks, leading to dramatic security concerns due to the scale and complexity of the system. Two major issues within this area are known as scalability and heterogeneity.

- As the IIoT's size and complexity are notably expanded, tackling security is dramatically difficult. Traditional solutions are showing their ages by its poor performance in handling scaling, potentially leading to cybersecurity attacks. In addition, controlling updates and patches across multitude of devices seems to be a challenging task, further complicated by the diversity of the IIoT ecosystem. Consequently, to create an effective and scalable IIoT security solution, it must be seamlessly capable of controlling an array of devices and protocols while making sure that all systems are up-to-date and secure.
- Another major challenge when it comes to IIoT is heterogeneity, which refers to the variety of devices, networks, protocols, and frameworks in the IIoT ecosystems. Such diversity could create interoperability concerns, which could lead to dramatic security leaks. For example, different manufacturers may use different protocols for their devices, causing compatibility and communication issues. Moreover, some devices may not be protected by advanced security measures, creating weak links within the security framework.

B. Guarding the security of Real-time monitoring [16]

As required by the internal nature of most IIoT applications, security approaches must not only protect devices from attacks but also track and respond to the user in real-time. While it is easy for a small volume of data, this would be complicated with large live-generated data volumes, making it difficult to detect suspected behaviour or intrusion.

- Solutions such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are slow to respond to real-time demands. Thus, an advanced monitoring solution that empowers AI and ML to detect and report security incidents live is essential.
- When a threat is detected, a fast and responsive mechanism to respond to the threat is essential. Mostly, due to the scale and sensitivity of operating times, human inspection for each detected breach is impractical. As a result, automated responses are needed, but they could cause false negative (positive) responses, which could let the intrusion easily fly through without being guarded.
- Although AI and ML are growing day by day, applying it to the cybersecurity field seems to be an impossible challenge. As most IIoT devices require resource-constraints, the AI model that is used for detecting intrusions must be lightweight, efficient, and able to handle large volumes of data in real-time.

V. Solutions for Unresolved Issues

To tackle the unresolved concerns in IIoT security, genius solutions are currently being researched in both academic and industrial contexts

A. Unified Frameworks [3] [4]

Multiple studies are currently underway in order to develop security frameworks that are unified and could be integrated into distinct IIoT standards. This consolidation pivots to simplify the integration process, enhance interoperability, and unify the security of different kinds of IIoT devices under a single framework. For example, NIST has published the Cybersecurity for IoT programme. This programme includes various publications, such as NISTIR 8228 and the mentioned NIST Cybersecurity Framework, which offer strategies to manage cybersecurity issues across different scenarios [4].

- Strengths: Unified security management; Increased interoperability.
- Weaknesses: Challenges in unifying different standards; Reluctance from stakeholders to adopt new standards; The potential to oversee the security needs of industry.

B. Lightweight Cryptographic Solutions [5] [6]

Aiming to provide a solution that satisfies the resource constraints of IIoT devices, significant number of researchers are focusing on developing a lightweight solution for cryptography. These solutions, aiming for less computational dependence and less energy-consumption, such as hash functions and lightweight block ciphers, are tailored for IIoT devices. For instance, Xinxin Fan and his team developed the WG-8 lightweight cipher, an alternative that targets devices with limited memory and computational resources, guarding the confidentiality and integrity of data while maintaining the unique constraints of IIoT environments [6].

- Strengths: Target resource-constrained systems; Ensure the confidentiality and integrity of data.
- Weaknesses: Potential advanced cryptographic vulnerabilities due to lightweight design.

C. Secure Lifecycle Management [7]

Nowadays, Blockchain is known as the technology that could protect lifecycle management for IIoT systems to increase transparency and accountability. The features of blockchain, which are decentralised and immutable, offer a secure and resistant lifecycle record of a device [7].

- Strengths: Increase transparency and accountability; Ensure resistant device history.
- Weaknesses: Require large resource for computing, which may not suit all IIoT devices; Vulnerabilities regarding scaling due to managing blockchain are complex procedures.

D. Fog and Edge Computing [8] [9]

Similar to Blockchain, Fog and Edge computing are decentralised frameworks designed for allowing data to be processed from source, which helps reduce latency and improve the performance of IIoT networks. These models can help minimise the demand for long-range data transmission by placing computational systems at the edge of the network, resulting in reduced latency, enhanced real-time responsiveness, and reduced vulnerabilities regarding data transmission. Moreover, with its decentralised nature, Edge Computing offers greater privacy by enabling the processing of data locally, thus eliminating the need for a central server to send data [8] and [9].

- Strengths: Improve real-time responsiveness; Greater privacy; Reduce latency.
- Weaknesses: Local data processing means local vulnerabilities, thus need for robust protection on edge devices; More challenges to managing the security of the network's edge.

The proposed approaches hold both promises and possible challenges regarding performance, cost, and operational conditions in the IIoT field. Researching and developing non-stop is essential to staying on-track with the newest threats and constraints in IIoT.

VI. Conclusions

The evolution of Industry 4.0 could not proceed without the Industrial Internet of Things (IIoT), which contributes to significant changes in industries. However, the transformation also brings a variety of security issues. This research has performed a deep analysis of these issues, examining the popular in-use IIoT Frameworks and Protocols, the vulnerabilities that these tools aim for, the unresolved vulnerabilities, and potential approaches.

Protocols such as MQTT, CoAP, and DDS, along with detailed frameworks like the IEC 62443 standard and the NIST Cybersecurity Framework, introduce strong defences against headache vulnerabilities. Nonetheless, issues related to scalability, heterogeneity, and secure real-time monitoring still remain, necessitating novel approaches.

New innovations and technologies, like Unified Frameworks, Lightweight Cryptographic Solutions, Secure Lifecycle Management, and Fog and Edge Computing, represent promise in addressing these unresolved vulnerabilities [3][4][5][6][7][8][9]. However, these approaches are not without their own challenges and limitations.

In conclusion, While the security of IIoT is continually updated with new technologies and advancing protocols, balancing it with performance, cost-effectiveness and good implementation is still a significant issue. Constant research, up-to-date upgrades to new protocols and frameworks, and a multi-layered approach are necessary to tackle IIoT breaches. Protecting the IIoT is a technical task that requires both understanding the potential issues and the current security solutions. The research enhances the understanding of the current IIoT landscape and offers directions insights for this essential field.

References

[1] H. Xu, W. Yu, D. Griffith and N. Golmie, "A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective," in *IEEE Access*, vol. 6, pp. 78238-78259, 2018, doi: 10.1109/ACCESS.2018.2884906.

[2] L. D. Xu, W. He and S. Li, "Internet of Things in Industries: A Survey," in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233-2243, Nov. 2014, doi: 10.1109/TII.2014.2300753.

[3] K. Megas, "NIST Cybersecurity for IoT," 2021. Accessed: May. 20, 2024. [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/nist-cybersecurity-for-iot-update/images-media/NIST%20%20Cybersecurity%20for%20IOT%20Update%20Megas.pdf#:~:text=URL%3A%20https%3A%2F%2Fcsrc.nist.gov%2FCSRC%2Fmedia%2FPresentations%2Fnist

[4] M. Fagan, "Cybersecurity for IoT: The Road We've Traveled, The Road Ahead," *NIST*, May 2022, Available: https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-iot-road-weve-traveled-road-ahead

[5] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Generation Computer Systems*, vol. 129, Nov. 2021, doi: 10.1016/j.future.2021.11.011.

[6] Fan, X., Mandal, K., Gong, G. (2013). "WG-8: A Lightweight Stream Cipher for Resource-Constrained Smart Devices". In: Singh, K., Awasthi, A.K. (eds) Quality, Reliability, Security and Robustness in Heterogeneous Networks. QShine 2013. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 115. Springer, Berlin, Heidelberg. 10.1007/978-3-642-37949-9_54.

[7] X. Guo, G. Zhang, and Y. Zhang, "A Comprehensive Review of Blockchain Technology-Enabled Smart Manufacturing: A Framework, Challenges and Future Research Directions," *Sensors*, vol. 23, no. 1, p. 155, Jan. 2023, doi: 10.3390/s23010155.

[8] T. Kim, S. Yoo, and Y. Kim, "Edge/Fog Computing Technologies for IoT Infrastructure," *Sensors*, vol. 21, no. 9, p. 3001, Apr. 2021, doi: 10.3390/s21093001.

[9] T. Kim, S. Yoo, and Y. Kim, "Edge/Fog Computing Technologies for IoT Infrastructure II," *Sensors*, vol. 23, no. 8, pp. 3953–3953, Apr. 2023, doi: 10.3390/s23083953.

[10] A. Al-Fuqaha, et al., "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," , IEEE Communications Surveys and Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015.

[11] K. Ware, "Understanding MQTT Security: A Comprehensive Overview," *www.emqx.com*, 2023. https://www.emqx.com/en/blog/understanding-mqtt-security-a-comprehensive-overview.

[12] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," *The Constrained Application Protocol (CoAP)*, Jun. 2014, doi: 10.17487/rfc7252.

[13] G. Pardo-Castellote, "OMG Data-Distribution Service: architectural overview," *23rd International Conference on Distributed Computing Systems Workshops, 2003.*

Proceedings., Providence, RI, USA, 2003, pp. 200-206, doi: 10.1109/ICDCSW.2003.1203555.

[14] B. Leander, A. Čaušević, and H. Hansson, “Applicability of the IEC 62443 standard in Industry 4.0 / IIoT,” *Proceedings of the 14th International Conference on Availability, Reliability and Security*, Aug. 2019, doi: 10.1145/3339252.3341481.

[15] D. P. F. Möller, “NIST Cybersecurity Framework and MITRE Cybersecurity Criteria,” *Advances in Information Security*, pp. 231–271, 2023, doi: 10.1007/978-3-031-26845-8_5.

[16] N. Sunanda, K. Shailaja, P. Kandukuri, Krishnamoorthy, V. S. Rao, and S. R. Godla, “Enhancing IoT Network Security: ML and Blockchain for Intrusion Detection,” *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 4, 2024, doi: 10.14569/ijacsa.2024.0150497.

[17] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, “A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures,” *Computers*, vol. 9, no. 2, p. 44, May 2020, doi: 10.3390/computers9020044.