Tackling Security in the Industrial Internet of Things: Current Frameworks, Unresolved Issues, and Emerging Approaches

1st Shaugato Paroi
Dept. Of Computer Science
Swinburne University Of Technology
Hawthorn, Australia
103523487@student.swin.edu.au

***Abstract*—The Industrial Internet of Things (IIoT) lies at the heart of Industry 4.0, introducing a myriad of benefits but also numerous security challenges due to its inherent characteristics and application environment. This report provides a comprehensive analysis of the security issues presented by the IIoT, focusing on current security frameworks and protocols, the problems they aim to resolve, the remaining unresolved issues, and prospective approaches to these challenges. We examine popular protocols such as MQTT, CoAP, and DDS, as well as frameworks like IEC 62443 and NIST Cybersecurity Framework, highlighting their efforts towards securing IIoT systems. However, significant challenges remain, particularly in terms of scalability and heterogeneity, and real-time security monitoring and response. Potential solutions including Fog and Edge Computing, Unified Security Frameworks, Lightweight Cryptographic Solutions, and Secure Lifecycle Management are discussed, providing insight into the future trajectory of IIoT security. This research underscores the dynamic nature of the IIoT security landscape, emphasizing the need for continued research and development in this area.**

***Index Terms*—Industrial Internet of Things (IIoT), IIoT Security, style, MQTT, CoAP, DDS, IEC 62443, NIST Cybersecurity Framework, Scalability and Heterogeneity, Real-time Security Monitoring and Response, Fog and Edge Computing, Unified Security Frameworks, Lightweight Cryptographic Solutions, Secure Lifecycle Management, 14. Industry 4.0**

I. INTRODUCTION

The Industrial Internet of Things (IIoT), a critical pillar of the Industry 4.0 revolution, has dramatically transformed traditional industries by integrating physical and digital systems, exploiting networking capabilities, and utilizing large-scale data analytics. However, while this paradigm shift comes with considerable benefits, it also brings forth new, complex security challenges that require rigorous and continual attention [1][2].

IIoT is characterized by its operation in potentially hazardous environments, control over dangerous machinery, and strict timing requirements, thereby demanding a unique set of security considerations. Furthermore, the large-scale and distributed nature of IIoT networks introduces a plethora of security vulnerabilities that adversaries can exploit to initiate both cyber and physical attacks [2][3].

This research report delves into these complex security issues presented by the IIoT, focusing on the relevant security frameworks and protocols developed to safeguard against them, the problems they aim to solve, and the critical unresolved security issues. It also explores potential approaches being considered to tackle the unresolved issues and enhance IIoT security.

We begin by detailing the security frameworks and protocols currently in use, such as MQTT, CoAP, and DDS, as well as comprehensive guidelines like the IEC 62443 standard and the NIST Cybersecurity Framework [7][8][9][10][11]. An in-depth evaluation of these tools uncovers the specific problems they are designed to solve, from secure and efficient data transfer to risk assessment and secure system design.

Despite the robustness of these protocols and frameworks, several significant issues remain unresolved, particularly concerning scalability and heterogeneity, and real-time security monitoring and response [15][16]. The research pivots to examining these unresolved issues, their implications on IIoT security, and the potential approaches to mitigating them. These include novel technologies and strategies like Fog and Edge Computing, Unified Security Frameworks, Lightweight Cryptographic Solutions, and Secure Lifecycle Management [18][19][20][22][23][24].

In addressing these points, this research report offers an in-depth, comprehensive analysis of IIoT security, contributing to the ongoing academic and industrial discourse. In the light of the complex and evolving nature of security challenges in IIoT, constant vigilance, research, and development are vital in securing this essential facet of Industry 4.0 [2][3].

II. SECURITY FRAMEWORKS AND PROTOCOLS:

Addressing the complex security requirements of the IIoT involves designing and implementing effective security frameworks and protocols. Several robust mechanisms have been proposed and are in use today, seeking to ensure secure communication, reliable operations, and data integrity in IIoT systems.

A. The Message Queue Telemetry Transport (MQTT)

MQTT protocol is one such commonly used protocol. MQTT, which was designed for lightweight message transfer, is widely used in IIoT due to its ability to efficiently handle high latency or unreliable networks, making it suited for remote industrial applications. MQTT, on the other hand, lacks natural security capabilities, necessitating the use of secure transport protocols such as TLS/SSL for encryption [7].

B. Constrained Application Protocol (CoAP)

Another IIoT protocol built for resource-constrained nodes is the CoAP. CoAP is lightweight and supports both request-response and publish-subscribe communication modes, making it applicable to a wide range of IIoT scenarios. It also offers security protections built in using Datagram Transport Layer Security (DTLS) [8]

C. DDS

DDS for real-time systems, on the other hand, concentrates on data-centric security and provides fine-grained security controls. DDS can secure data both in transit and at rest, making it a viable security mechanism for real-time industrial applications where timely access to reliable data is critical [9].

D. International Electrotechnical Commission's IEC 62443

As for security frameworks, the International Electrotechnical Commission's IEC 62443 standard provides comprehensive guidelines for securing Industrial Control Systems (ICS). It covers multiple aspects of ICS security, from system design to deployment and maintenance, including risk assessment, system architecture design, and secure product development [10].

E. National Institute of Standards and Technology (NIST)

Similarly, the Cybersecurity Framework from the National Institute of Standards and Technology (NIST) provides a flexible and customizable approach for managing cybersecurity risks in IIoT. It is composed of five core functions – Identify, Protect, Detect, Respond, and Recover – that cover various aspects of cybersecurity from threat identification to mitigation and recovery [11].

III. Targeted Problems of the Frameworks and Protocols:

The assortment of protocols and frameworks discussed in the context of IIoT were developed to address several specific challenges arising from the unique characteristics and constraints of the IIoT landscape. These challenges encompass reliable and secure data transmission, system integrity, device authentication, privacy protection, and coping with resource-constrained devices.

An in-depth look at the targeted problems by each protocol is as follows:

A. Unreliable or High-latency Networks

MQTT, or Message Queuing Telemetry Transport, has been specifically designed to operate over unreliable or high-latency networks. Its pub-sub model allows for efficient distribution of messages, reducing the demand for network bandwidth and reducing latency. The client and broker model eliminates the need for constant connections, further enhancing its performance in these challenging network conditions. Moreover, it uses a three-level QoS mechanism to ensure message delivery reliability under various network conditions.

B. Resource-Constrained Nodes and Security

The Constrained Application Protocol (CoAP) was designed to operate with resource-constrained nodes and networks, providing a lightweight alternative to HTTP. It employs a RESTful architecture, using simple methods like GET, POST, PUT, and DELETE to interact with resources, which can be uniquely identified by URIs. CoAP also incorporates DTLS (Datagram Transport Layer Security) for secure communication, protecting data integrity and confidentiality, and providing optional endpoint authentication.

C. Real-time Data Security

The Data Distribution Service (DDS) prioritizes data-centric security, taking a real-time systems approach. By supporting fine-grained security settings, DDS can provide access control at the data level, only allowing authorized entities to access specific data. This is crucial for industrial applications where certain data should be restricted to specific users or systems. Moreover, DDS encrypts data in transit, which ensures that even if data is intercepted, it cannot be understood, thereby maintaining its integrity and confidentiality.

D. Overall ICS Security

This standard provides a comprehensive framework for securing industrial automation and control systems. It adopts a full lifecycle view, providing guidance from the design to the maintenance phase. This includes system requirements definitions, system design, implementation, installation, operation, maintenance, and decommissioning. The defense-in-depth model is central to the framework, providing multiple layers of security. This holistic approach ensures that a weakness in one area does not compromise the entire system.

E. Cybersecurity Management

The NIST Cybersecurity Framework provides a high-level, strategic approach to managing cybersecurity risk. It promotes awareness and understanding of cybersecurity risk at all levels of the organization, ensuring that all stakeholders are engaged in managing the risk. The framework is divided into five core functions: Identify, Protect, Detect, Respond, and Recover. These functions provide a high-level taxonomy of cybersecurity outcomes, and they organize foundational cybersecurity activities at their highest level. These functions also aid in expressing cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

Each of these protocols and frameworks provides crucial tools and guidance in tackling the security challenges present in the IIoT landscape.

IV. Unresolved Issues:

While the current security frameworks and protocols have achieved significant strides in securing the IIoT landscape, several issues remain unresolved. The unresolved issues identified from the can be consolidated into two major concerns:

A. Scalability and Heterogeneity [15][16][17]:

IIoT comprises a diverse array of devices, networks, standards, and protocols. The sheer scale and complexity of these systems pose significant security challenges. Two prominent concerns within this area are heterogeneity and scalability.

- Heterogeneity implies the variety of devices, networks, protocols, and standards in IIoT systems. Such diversity leads to interoperability issues, which can have severe security implications. For example, devices from different manufacturers may use distinct security protocols, potentially leading to compatibility issues and communication breakdowns. Some devices might not be equipped to handle advanced security measures, creating weak links in the security chain.
- Scalability is another major challenge. As the size and complexity of the IIoT grow, managing security becomes increasingly challenging. Traditional security solutions might not scale well, leading to potential vulnerabilities. Moreover, managing security updates and patches across a large number of devices is a daunting task that becomes even more complicated when considering the heterogeneous nature of the IIoT ecosystem. A scalable and effective IIoT security solution would need to seamlessly handle a multitude of devices and protocols while ensuring that all components are updated and secure.

B. Real-time Security Monitoring and Response [18][19][20]:

Due to the critical nature of many IIoT applications, security solutions must not only prevent breaches but also detect and respond to them in real-time. This is complicated by the large volume of data generated by IIoT devices, making timely detection of anomalous behavior or intrusion attempts difficult.

- Current solutions like IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems) still struggle to keep up with the real-time demands of IIoT systems. There is a need for advanced security monitoring solutions capable of leveraging AI and machine learning techniques to swiftly detect and react to security incidents.
- Despite the advancements in AI, implementing them in IIoT for security purposes is still a challenge due to the resource-constrained nature of many IIoT devices. The models used for anomaly detection or intrusion detection should be lightweight yet effective, able to process high volumes of data in real-time, which is a non-trivial task.
- Also, once a threat is detected, there needs to be a quick and effective response mechanism. In many cases, human intervention for each detected threat would be impractical due to the scale and time-sensitivity of operations. As such, automated response mechanisms are essential, but they come with the challenge of avoiding false positives and negatives, which can disrupt the operation of the IIoT system or let threats slip through undetected.

V. Approaches to Unresolved Issues:

To address the unresolved issues in IIoT security, several innovative approaches are currently being explored in the academic and industrial realms.

A. Fog and Edge Computing [21][23]:

Fog and Edge computing are decentralized models that enable data processing at the data source, aiming to reduce latency and improve the efficiency of IIoT networks. By placing computational resources at the network's edge, the need for long-distance data transmission is reduced, thereby decreasing latency, improving real-time responsiveness, and potentially mitigating vulnerabilities associated with data transmission. Edge computing can also provide additional privacy, as local data processing can eliminate the need to transmit data to a central server [23].

- Strengths: Reduced latency, increased privacy, and improved real-time responsiveness.
- Weaknesses: Greater complexity in managing security at the edge of the network, potential for localized vulnerabilities, and a need for robust edge device protection.

B. Unified Frameworks [19]:

Research is active towards developing unified security frameworks to integrate diverse IIoT standards. This consolidation aims to streamline the integration of various standards to enhance interoperability and simplify securing diverse IIoT devices under a single framework. For example, the Industrial Internet Consortium (IIC) aims to define a comprehensive security framework that provides a consistent approach to IIoT security across various sectors [19].

- Strengths: Enhanced interoperability, streamlined security management.
- Weaknesses: Difficulties in harmonizing diverse standards, resistance from stakeholders to adopt new standards, potential for overlook of specific industry or device security needs.

C. Lightweight Cryptographic Solutions [20][24]:

With the resource constraints of many IIoT devices in mind, significant research focuses on developing lightweight cryptographic solutions. These less computationally demanding and energy-consuming methods, such as lightweight block ciphers and hash functions, are more suitable for IIoT devices. For example, the National Security Agency (NSA) has developed lightweight cryptographic algorithms SPECK and SIMON, designed for resource-constrained environments [24].

- Strengths: Suitable for resource-constrained devices, maintains data confidentiality and integrity.
- Weaknesses: Possible compromises in cryptographic strength due to lightweight design, potential vulnerabilities to advanced cryptographic attacks.

D. Secure Lifecycle Management [22]:

Blockchain technology is being considered for secure lifecycle management of IIoT devices to enhance transparency and accountability. Blockchain's decentralized and immutable nature could provide a secure and tamper-proof record of a device's lifecycle from manufacture, deployment, updates, and eventual decommissioning [22].

- Strengths: Enhances transparency, provides tamper-proof device history.
- Weaknesses: Requires considerable computational resources which may not be suitable for all IIoT devices, potential scalability issues, the complexity of blockchain management.

These approaches indeed hold promise, but substantial challenges persist in balancing the demand for security with performance, cost, and operational considerations within the IIoT context. Continued vigilance, research, and development are imperative to keep pace with the evolving threat landscape and unique IIoT constraints.

VI. Conclusion

TThe Industrial Internet of Things (IIoT) plays a pivotal role in driving the fourth industrial revolution, known as Industry 4.0. However, this digital transformation also introduces a variety of intricate and multi-faceted security issues. This report has performed a thorough analysis of these complexities, examining the current security frameworks and protocols in use, the targeted problems they resolve, the major unresolved issues, and the prospective approaches towards these remaining challenges.

Security protocols like MQTT, CoAP, and DDS, alongside comprehensive frameworks such as the IEC 62443 standard and the NIST Cybersecurity Framework, provide a robust defense against several vulnerabilities in IIoT systems [7][8][9][10][11]. Nonetheless, the issues of scalability and heterogeneity and real-time security monitoring and response remain persistent, demanding novel solutions [15][16].

Emerging technologies and methodologies such as Fog and Edge Computing, Unified Security Frameworks, Lightweight Cryptographic Solutions, and Secure Lifecycle Management represent promising approaches towards these unresolved issues [18][19][20][22][23][24]. However, they are not without their own challenges and limitations.

As this report underlines, the security landscape of the IIoT is a dynamic one, continually evolving as new technologies emerge, and threats advance. Balancing security with operational performance, cost-effectiveness, and practical implementation remains a significant challenge. It is evident that continual research and development, timely updates to protocols and frameworks, and a multi-layered security approach are necessary to address the sophisticated threats faced by the IIoT.

In conclusion, securing the IIoT is an ongoing task that requires an understanding of both the potential risks and the available security measures. This research contributes to the understanding of the current state of IIoT security, offering insights into the potential directions for future work in this critical area.

References

[1]] L. Da 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.

[2] G. Tsagkaris, et al., ”From the Internet of Things to the Internet of People”, IEEE Internet Computing, vol. 19, no. 2, pp. 40-47, 2015.

[3] 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.

[4] E. Byres, ”Using ANSI/ISA-62443 Standards to Secure Your Industrial Control Systems”, ISA Whitepaper, 2019.

[5] M. M. Rathore, A. Paul, ”Industrial Internet of Things: Challenges, Issues and Solutions”, IEEE Access, vol. 7, pp. 77958-77978, 2019.

[6] L. Xiao, et al., ”A Survey of Distributed Consensus Protocols for Internet of Things”, IEEE Access, vol. 6, pp. 1504-1524, 2018.

[7] H. Truong, et al., ”Security Challenges in Integration of Cloud Computing and Internet of Things”, in 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2019, pp. 295-300.

[8]] Z. Shelby, et al., ”The Constrained Application Protocol (CoAP)”, Internet Engineering Task Force (IETF), RFC 7252, Jun. 2014.

[9] G. Pardo-Castellote, ”OMG Data-Distribution Service: Architectural Overview”, in 23rd International Conference on Distributed Computing Systems Workshops, 2003, pp. 200-206.

[10] International Electrotechnical Commission, ”IEC 62443: Security for industrial automation and control systems”, 2020.

[11] National Institute of Standards and Technology, ”Framework for Improving Critical Infrastructure Cybersecurity”, Version 1.1, 2018.

[12] S. R. Moosavi, et al., ”Lightweight security solutions for the Internet of Things”, in 2016 IEEE International Conference on RFID (RFID), 2016, pp. 1-7.

[13] H. Duan, et al., ”Everything You Want to Know About the Blockchain: Its Promise, Components, Processes, and Problems”, in IEEE Transactions on Industrial Informatics, vol. 14, no. 7, pp. 3282-3296, July 2018.

[14] M. Wollschlaeger, et al., ”The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0”, in IEEE Industrial Electronics Magazine, vol. 11, no. 1, pp. 17-27, March 2017.

[15]] N. Kshetri, ”Can Blockchain Strengthen the Internet of Things?”, in IT Professional, vol. 19, no. 4, pp. 68-72, July/August 2017.

[16] A. Ahmad, et al., ”Security in the Internet of Things: Uncover the Challenges and Solutions”, in 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), 2018, pp. 108-113.

[17] K. Zhao, et al., ”A Survey of the Internet of Things Security: Requirements, Attacks, and Countermeasures”, in IEEE Communications Surveys and Tutorials, vol. 20, no. 4, pp. 3452-3471, Fourthquarter 2018.

[18] P. Garcia Lopez, et al., ”Edge-centric Computing: Vision and Challenges”, in ACM SIGCOMM Computer Communication Review, vol. 45, no. 5, pp. 37-42, 2015.

[19] Industrial Internet Consortium, ”Industrial Internet Security Framework Technical Report”, 2016.

[20] A. Bogdanov, et al., ”PRESENT: An Ultra-Lightweight Block Cipher”, in CHES 2007, LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007).

[21] J. Kim, et al., ”A Novel Approach to Intrusion Detection Systems for the Internet of Things by Using Lightweight Secure SDN”, in IEEE Access, vol. 7, pp. 41623-41633, 2019.

[22]] N. Kshetri, ”1 Blockchain's roles in meeting key supply chain management objectives”, International Journal of Information Management, vol. 39, pp. 80-89, 2018.

[23] S. Yi, C. Li, Q. Li, ”A Survey of Fog Computing: Concepts, Applications, and Issues”, Proceedings of the 2015 Workshop on Mobile Big Data. Mobidata ’15. pp. 37–42, 2015.

[24] R. Beaulieu, et al., ”The SIMON and SPECK Families of Lightweight Block Ciphers”, Cryptology ePrint Archive, Report 2013/404, 2013.