ICAI 2023
12th International Conference on Applied Informatics
Eger, Hungary, 2023

Cloud and On-Premises based security solution for Industrial IoT

Orkhan Aslanli

Faculty of Informatics, University of Debrecen
orkhan@mailbox.unideb.hu

Abstract

The Internet of Things (IoT) has initially been defined as an ecosystem of interconnected smart devices. Today, the improvements in smart devices allow people to utilize them in different fields. For that reason, we can mention that the scope of IoT ranges widely in different fields, such as smart homes, healthcare, the automotive industry, etc. As we mentioned, the utilization of IoT is increasing dramatically, and those devices are becoming the main target of cyber-criminals. They are manipulating the data, which is crucial for the built ecosystems.

In this paper, we take Industrial IoT as a primary point, where we touch on the direction of Industrial IoT concepts and connectivity protocols used by Industrial IoT devices. Moreover, we go in deeply security challenges that where Industrial ecosystem faces. As we know, today, most industries are being focused on specific protocols in their smart IoT devices. In return, we mainly focus on Message Queuing Telemetry Transport (MQTT) protocol, MQTT servers to which IoT devices are connected, and secure connectivity among server, cloud, and end user. Our purpose here is to describe the security approach for server and cloud-based environments and the utilization of cloud security tools such as segmentation of zones, load balancers, and cloud-based Load balancers. In detail, if we think widely when designing the system, proper steps are considered to utilize the appropriate device, build a threat model to understand how an attacker could be able to compromise the ecosystem, and the segmentation principle for the planned IoT ecosystem.

After the discussion of the infrastructure, we concern how to choose proper IoT devices which give extra security features. Next, we describe how to build a threat model with the best security practices that give a well-prepared understanding of cyber-attacks. Afterward, we consider that, as a part of security practice,

segmentation plays a vital role in having a secure ecosystem. With reference to segmentation, we focus on what should be deemed and what are the benefits of segmentation – such as devices, field gateways, and cloud services. Finally, we focus on possible cloud security services that give the opportunity to secure the whole ecosystem and have high performance.

Keywords

Internet of things, Azure Cloud, Security threats, Cloud Security Monitoring, Industrial IoT ecosystems, IoT connectivity protocol

References

[1] Björn Leanderr and Hans Hansson, "Cybersecurity Challenges in Large Industrial IoT Systems," *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA).*, 2019

[2] Zeinab Bakshi, Ali Balador and Jawwad Mustafa, "Industrial IoT Security Threats and Concerns by Considering Cisco and Microsoft IoT reference Models," *IEEE Wireless communication and Networking Conference Workshops.*, 2018

[3] Hanlin Chen, Ming Hu, Hui Yan and Ping Yu, "Research on Industrial Internet of Things Security Architecture and Protection Strategy," *IEEE International Conference on Virtual Reality and Intelligent system.*, 2019

[4] George Mavridis, "Security Mechanisms for Internet of Things," *Academia.edu.*, 2021

[5] Lubna Luxmi Dhirani, Eddie Armstrong and Thomas Newe, "Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap," *IEEE Wireless communication and Networking Conference Workshops.*,2021

[6] Joseph Jose Anthraper, Jaidip Kotak, "Security, Privacy and Forensic Concern of MQTT protocol," *International Conference on Sustainable Compiting in Science.*, 2019

[7] Jiong Shi Liping Jin and Jun Li, "The Integration of Azure Sphere and Azure Cloud Services for Internet of Things," *MDPI.*, 2018

[8] Abhijeet Thakare, Euijong Lee, Ajay Kumar, Valmik B Nikam and Young-Gab Kim, " PARBAC: Priority-Attribute-Based RBAC Model for Azure IoT Cloud," *IEEE Wireless communication and Networking Conference Workshops.*, 2019

[9] Luigi Coppolino, Salvatore, D' Antonio, Giovanni Mazzeo and Luigi Romano, "Cloud security: Emerging threats and current solutions," *Computers and Electrical Engineering.*,2017

[10] Haralambos Mouratidis, Vasiliki Diamantopoulou, "A Security Analysis Method for Industrial Internet of Things," *IEEE Transaction and Industrial Internet of Things.*, 2018

[11] Michael Frey, Cenk Gundogan, Peter Kietzmann, Martine lenders, Hauke petersen, Thomas C. Schmidt, Flex Juraschek, Matthias Wahlisch, "Security for the Industrial IoT: The Case for Information-Centric Networking," *IEEE 5th World Form on Internet of Things.*,2018

[12] Martin, Serror, Sacha Hack, Martin henze, Marko Schuba and Klaus Wehrle, "Challenges and Opportunities in Securing the Industrial Internet of Things," *IEEE Transaction on Industrial Informatics.*, 2018

[13] Soo Fun Tan and Azman Samsudin, "Recent Technologies, Security Countermeasure and Ongoing Challenges of Industrial Internet of Things (IIoT): A Survey," *MDPI.*, 2021

[14] Ahmad Reza Sadeghi, Christian Wachsmann and Michael Waidner, "Security and Privacy Challenges in Industrial Internet of Things," *IEEE Wireless communication and Networking Conference Workshops.*, 2018