I.J. Information Engineering and Electronic Business, **2024, 5, 55-62**
Published Online on October 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2024.05.02

Cloud and On-premises Based Security Solution for Industrial IoT

Orkhan Aslanli*
University of Debrecen, Theoretical computer science, data security and cryptography, Debrecen, 4028, Hungary
E-mail: orkhan@mailbox.unideb.hu
ORCID iD: https://orcid.org/0009-0003-4312-5356
*Corresponding Author

Received: 07 January, 2024; Revised: 23 February, 2024; Accepted: 19 March, 2024; Published: 08 October, 2024

Abstract: In this paper, we take Industrial IoT (IIoT) as a main point, where we touch on the direction of Industrial IoT concepts and connectivity protocols used by Industrial IoT devices. Moreover, we go into deep security challenges the Industrial ecosystem faces. Nowadays, most industries focus on specific protocols in their smart IoT devices. In return, we mainly focus on Message Queuing Telemetry Transport (MQTT) protocol, MQTT server where IoT devices are connected to it, 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 IoT-hub, Network Security Group (NSG) and virtual private network (VPN). In more detail, here we have indicated proposed solution by separating into device, on-premises and cloud zone sections, proper technologies which are being used in modern security approaches and comparison with traditional IoT security approaches. This article enables readers to obtain fundamental knowledges on available technologies which are utilized in industrial areas and real-time scenarios where this solution is deployed.

Index Terms: Azure Cloud, Cloud security monitoring, Industrial IoT (IIoT), Threat Model, Network security group (NSG), Virtual network (Vnet).

1. Introduction

The Internet of Things (IoT) is rapidly growing, and it causes an increase in the ecosystem of connected devices, sensors, and smart machines that are all capable of collecting and sharing data between them and the end-users over the internet. IoT devices can be varied from simple sensors such as temperature, air pressure, and humidity to complex smart devices utilized in industrial connectivity. These IoT devices have the potential to adopt a new era of efficiency, productivity, quality, etc. If we have a quick look at technological development in different areas, we will observe that the adoption of IoT provides a huge number of benefits for humans. In particular, the application of industrial IoT offers a wide range of benefits for industrial ecosystems, such as the following.

- *Efficiency improvement: Industrial Internet of Things (IIoT) improves the efficiency of industrial operations by deploying automation of processes, decreasing manual labor, resulting in faster and more accurate production and lower downtime.*
- *Predictive Maintenance: IIoT devices collect data about equipment performance and health and provide precise timing when maintenance is needed. In return, it provides the industry with an advantage in reducing downtime and maintenance costs.*
- *Improved Quality Control: With the help of sensors, the industry can monitor production processes and detect any defect before a product goes to market.*

However, the widespread deployment of IIoT devices also brings significant security risks that must be solved to prevent potential attacks on the overall IIoT ecosystem. These risks can vary from financial loss to death or injuries and should be considered as an impact of security threats and cyber-attacks on Industrial IoT ecosystems. From another point of view, proper security solutions are required to securely build IIoT environments. One example of security challenges IIoT faces today is that we can consider connections between all components of IIoT environments, such as physical and cyber levels [1]. For example, if we consider the device zone, devices can be the victim of attacks by having physical access, in which an attacker can change the device to get access to the IoT network and exploit the sensitive data. In responding to these types of challenges, IIoT must be secured in a proactive manner. Therefore, in this

paper, we discuss cloud- and on-premises based IIoT concepts and list the benefits and connectivity protocols that are being used in the industry. In terms of security solutions, we propose our IIoT connectivity model and investigate the security approach starting from device to cloud.

2. Cloud versus on-premises Based Iiot Concept

IIoT is the utilization of connected devices and sensors that enable data collection and analysis of the data in the industrial environment. Nowadays, a wide number of enterprises tend to utilize IIoT devices, such as temperature, motion, humidity, and corrosion sensors in different areas. In return, these deployments provide great advantages for businesses and enterprises. After the evolution of cloud technologies, many companies are adopting the most recent cloud services, such as Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP), in their IoT-enabled ecosystem. In return, this direction provides benefits such as having remote access to data and applications, scalability, flexibility, and real-time monitoring [2].

On the other hand, deployment of an on-premises solution provides several benefits, such as the following:

- *Helps to improve data security: On-premises solutions help the industry maintain full control over their sensitive data and security protocols.*
- *Reduces latency: As we know, cloud solutions rely on internet connectivity, whereas on-premises solutions help reduce the time for data processing and real-time applications.*
- *Less dependence on the internet: This solution reduces the dependencies on internet connectivity, which can be undesirable in some use cases according to the deployed environment.*

Following figure 1 illustrates the IoT connectivity model based on 4 layers [3].

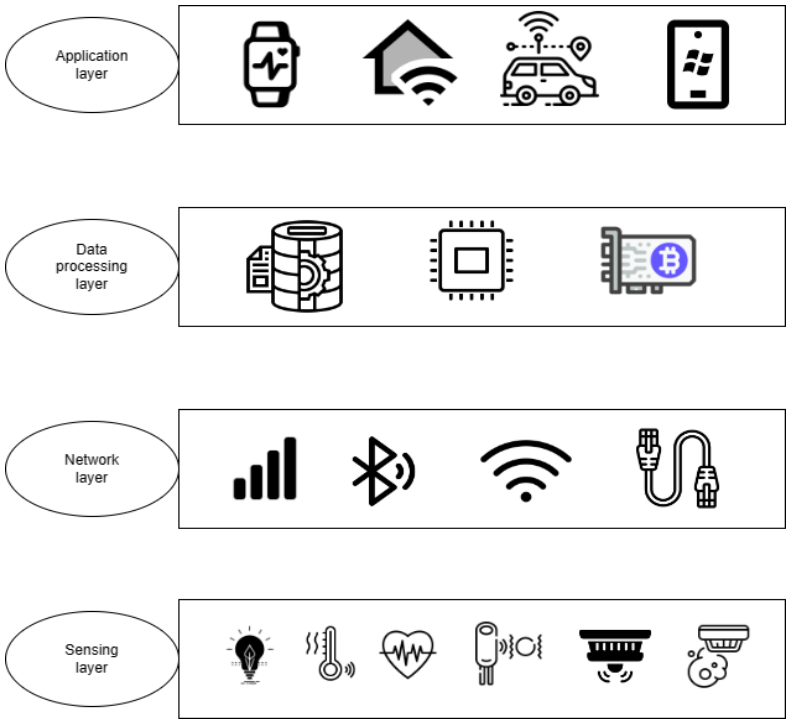


Fig. 1. IoT connectivity layers

3. Industrial IoT connectivity protocols

Connectivity protocols play a crucial role in IoT connectivity for enabling IoT devices to communicate with each other and with end-users as well. In this section, we are going to explore some of the most frequently used protocols in IIoT connectivity.

3.1. Message Queuing Telemetry Transport (MQTT)

MQTT protocol is known as a lightweight and efficient messaging protocol that was designed for resource-constrained devices that are limited with less bandwidth, high network latency, and low power [4]. There are several reasons why MQTT is one of the most used connectivity protocols in Industrial IoT ecosystems.

- Lightweight and efficient.
- Easy to implement.
- Reliable.
- Flexible.

3.2. Modbus

This protocol is open access for individuals in diverse domains without any associated fees. It has gained popularity as a connectivity protocol due to several noteworthy characteristics. Its simplicity is a primary factor contributing to its widespread adoption in various deployments. Additionally, another key attribute is its compatibility with industrial automation, particularly for communication between Programmable Logical Controllers (PLC) and various industrial devices. The protocol is structured on a master-slave architecture, where a master device can request data from one or multiple slave devices. Moreover, it is well-suited for low cost and dependable communication in Industrial IoT applications.

3.3. Constrained Application Protocol (CoAP)

The CoAP protocol is tailored for environments with resource-constrained devices. Like the MQTT protocol, it is a lightweight solution that facilitates effective communication among IoT devices. CoAP follows an HTTP-based structure, offers a request and response framework, and accommodates both uni-cast and multi-cast communication. These characteristics contribute to its widespread adoption [5].

3.4. Data Distribution Service (DDS)

It is not possible to avoid mentioning that the DDS protocol is also one of the popular protocols being used in industrial IoT connectivity. Its architecture is based on the publish subscribe method. This protocol enables scalable, real-time data distribution in complex IoT connectivity. There are several use cases for this protocol, such as it can be utilized in energy systems to manage and optimize the distribution of energy by integrating different types of monitoring tools. Altogether, it is suitable for managing complex data distribution in various IIoT systems by enabling real-time integration.

3.5. PROFINET

Similarly to the DDS protocol, the PROFINET protocol is widely used in the industrial IoT ecosystem, which enables real-time communication among industrial smart devices and automation systems. This protocol has several advantages while designing an Industrial IoT ecosystem, including integrated safety, motion control, and remote monitoring. In addition, this protocol comes with built-in security features that can encrypt and authenticate data to ensure integrity and confidentiality when data is transmitted over the network. Overall, this protocol is suitable for a wide range of industrial use cases, from manufacturing to energy.

4. Industrial IoT Security Challenges

Industrial IoT changes traditional industry operations by deploying various IoT devices, enabling industries to have real-time data insight, high-level automation, and increased efficiency. Although there are lots of benefits to integrating IoT technologies, these benefits also come with several security challenges that must be addressed. Below, we have listed current IIoT security challenges [6 - 8].

One of the main security challenges is the lack of standardized security protocol: If we compare the traditional IoT environment with modern IIoT, we will recognize that modern IIoT was not often designed with security in mind [9]. So, when designing an IIoT deployment, the ecosystem may lack standardized security protocols, making it challenging to secure them against any attack.

Another security challenge is the consideration of vulnerable devices: A huge number of vendors are producing different types of IIoT devices with various features. These devices may have limited computing power and security features, making them vulnerable to cyber-attacks.

The next security challenge is the physical security of IIoT devices: IIoT connects different types of devices and machines to the internet for data delivery. This connection enables attackers to access the built system and exploit vulnerabilities in these ecosystems to cause damage, disrupt operations, and steal sensitive data.

IIoT devices collect a large amount of data about industrial processes, and this data can be sensitive. This data must be protected from unauthorized access and data modification. In addition, sharing data across multiple organizations might increase the risk of exposing sensitive data to unauthorized access.

Device authentication is also considered one of the security challenges. It involves strong authentication protocols such as digital certificates and other forms of security approach. For example, by default, each device within the system is vulnerable to unauthorized access or tampering. For this reason, these devices should be verified and identified on the server's side where they transmit the data. It enables a server to obtain data only from authenticated and verified devices.

Overall, IIoT security challenges are complex. To address these challenges, industries, manufacturers, and vendors should carry out coordinated efforts to secure an IIoT ecosystem. In addition, organizations should invest in security training for employees to ensure safety and security in their daily operations [10].

5. Proposed IIoT Security Model

IIoT is a network of connected devices and machines that enable the industry to automate processes, real-time monitoring, and data analysis within the built smart ecosystem. In Figure 2, we have illustrated the sensor-to server, server-to-cloud, and cloud-to-end user model. This model contains sensors that are MQTT enabled and a server between IoT devices and data consumers.

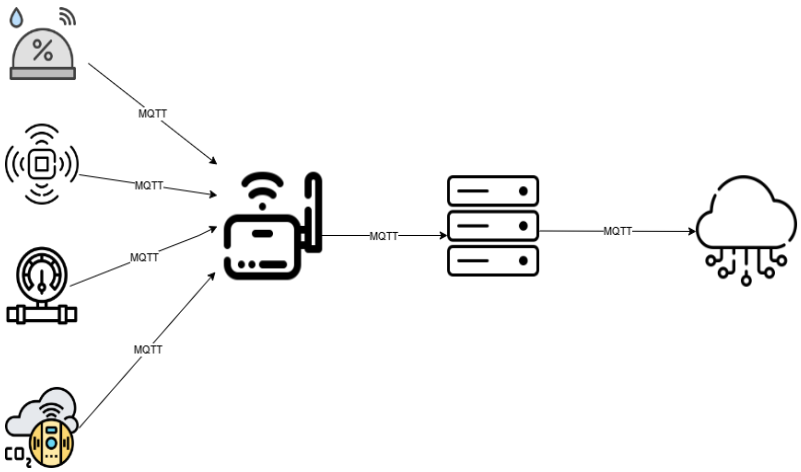


Fig. 2. IIoT connectivity model.

In this part, we provide a security solution according to Figure 2 to enhance the security approach by segmenting the design into device, server, and cloud zones.

5.1. Proposal for choosing components of the suggested security model.

Starting with the device type, here we consider the utilization of constrained sensors where they are power restricted. The reason for starting with low-level devices is that, in many cases, small industries focus on accommodating them to decrease the cost of building the intended IIoT ecosystem. Those devices are the most vulnerable to cyber-attacks.

In addition, deploying cloud and on-premises solutions gives us more flexibility: crucial data can be stored on premises, and less important ones can be delivered to the end user through cloud integration. As a result, we can have a more granular security approach for the data we obtain from the sensors. Moreover, cloud integration offers many opportunities to defend the data from unauthorized users.

5.2. Threat Model

A threat model for IIoT security involves identifying and assessing potential threats that can affect the overall security of the built industrial ecosystem. It helps organizations to understand the risks associated with their built IIoT deployment and improve actions against new security risks. In order to have a systematic approach to securing any IoT enabled ecosystem, the first essential step is to generate a threat model for the planned system. The corresponding threat model, according to our model, contains the following.

- *The architecture of the proposed system: The overall architecture of the system should be carefully considered by including the types of sensors and devices used in the framework.*
- *Data types and their sensitivity level: The sensitivity of the collected and generated data should be studied before data goes to the end user.*
- *Attack Surface: Determination of potential entry points to the system should be defined and restricted against unauthorized access.*
- *Evaluation of Threat Scenarios: Different threat scenarios should be reviewed according to the sensor, server, and cloud environment.*
- *Mitigation strategies: Security admins should overview network segmentation, access control, data encryption, and personnel training and awareness.*
- *Application of monitoring tools: Best-fit monitoring tools should be defined, and regular monitoring should be conducted to identify any possible new risks before they occur.*

5.3. Device security

Having a closer look at Figure 2 here, we can identify the main reason for choosing MQTT-enabled sensors as using MQTT protocol security features, for instance, Transport Layer Security (TLS) or Secure Sockets Layer Security (SSL) protocols and MQTT protocol is compatible with many constrained devices [11]. Utilization of these features allows us to encrypt messages between server and device. In addition, one of the best practices in network security is the segmentation of the structure. It lets us split the main network into multiple ones based on the types of data passing through. Each network zone represents an additional security layer with its access point [12]. That is why it is advised to use network segmentation as an initial step while building IIoT ecosystem. Implementation of this security approach gives the following benefits[13,14].

- *Minimizes the attack surface.*
- *Decreases the impact of an attack.*
- *Enables more granular security control.*
- *Compliances enhancement.*
- *Simplifies troubleshooting capability.*
- *Improves monitoring and threat detection.*
- *Protects endpoint devices.*

5.4. Server security

As one can see in Figure 2, a server is located between sensors and the cloud zone. Using an additional server as a data broker is recommended to enhance security measures. It provides the following security benefits.

- *Using Virtual Private Networks (VPN): It is well known that an MQTT broker is responsible for routing messages between clients and tracking authorized clients who subscribe to the message. In our case, VPN adds an extra layer for securing sensitive data by encrypting all traffic between the client and broker.*
- *Implementation of Firewalls: The main function of the broker is to receive and process messages from end users and devices. Setting the broker behind a firewall will limit access and make it more difficult for an unauthorized user to connect. To enhance broker security, TLS or SSL certificates should be used.*
- *Application of Access Control Lists (ACL): Identifying a proper ACL list and implementing the ACL file into a broker will allow only authorized users in the access list to receive or publish data [15].*
- *Identification of authorized devices: By identifying all deployed MQTT-enabled IoT devices, we can connect them to the data broker. On the data broker side, we can authorize them, and as a result, the data broker can only get data from licensed devices. This approach protects the system from any physical attack where an attacker has installed its own devices to gain access to the server.*

5.5. Cloud zone security

In this section, we regard Azure Cloud as a reference, and its connectivity and security features are suitable for our model. Microsoft Azure Cloud for IoT provides an Azure IoT Hub as a cloud gateway to accept data from the devices with increased security [16]. Another feature of the IoT hub is its native integration with other services. In addition, according to our scenario, the devices are MQTT enabled, and the IoT Hub supports MQTT data communication protocol. Figure 4 describes the above-mentioned connectivity model.

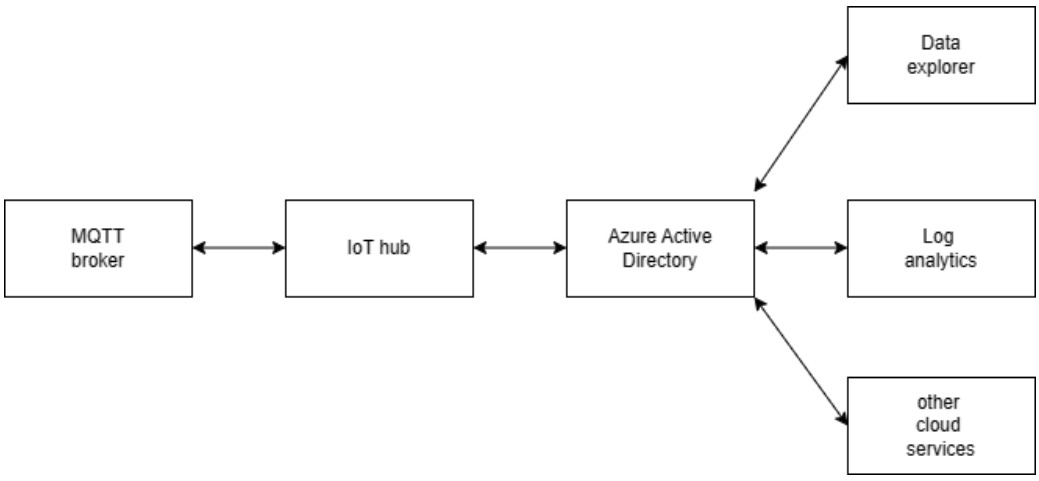


Fig. 3. Cloud connectivity

Implementation of shared access policies: To control access to IoT Hub resources, shared access policies give several benefits.

- *Improved security: This allows us to limit the permissions of users and devices.*
- *Granular Access Control: Regarding the level of devices, it enables defining different permissions.*
- *Simplified device management: Allows cloud admin to manage access to devices and modules from a single location.*
- *Scalability and flexibility: Helps to manage many devices and can be customized according to the needs of an IIoT system.*

Several mechanisms must be implemented to significantly decrease DoS or DDoS [17] attacks on the Azure IoT hub. By default, the front-end connection to the IoT hub is public, which means that this connection is accessible from the internet. To secure this connection, one of the best practices is the application of a Network Security Group (NSG). After applying NSG to the front-end connection of the IoT hub, we can control the inbound traffic to the hub from devices, and it will help us protect the IoT cloud from DDoS and any other attacks[18].

The next step after the application of NSG is to use private endpoints. Private endpoints are the IP addresses within your virtual network and enable secure access to specific Azure services such as storage, Time Series Insight, or Azure Cosmos DB. By implementing a private network, we can keep sensitive data within virtual network (Vnet) [19]. Moreover, Azure Active Directory integration should be completed to have control over users of the services. Thus, only authorized users can have access to cloud services [20].

The last step is security management. Here, Azure Cloud provides Azure Security Center, which enables unified security management across resources and high-level protection for the cloud environment, including the IoT Hub. In addition, it allows cloud security investigators to detect and respond to security threats in real-time.

5.6. Advantages of proposed hybrid solution against traditional IIoT security systems.

Hybrid industrial architecture enables organizations to build and manage connections to the industrial infrastructure. This architecture provides secure and reliable options to build ecosystems with operational environment. By combining both on premises and cloud applications, industrial organizations can collect data from multiple IoT sources and bring into one trusted secure system [21]. Moreover, continuous, automatic device and application monitoring systems become integrated and in return, it allows users to implement powerful safeguards to predict and prevent destructive malware attacks.

On the other hand, compared to traditional IIoT security, integration of cloud and on-premises solution for securing the industry, enables following benefits.

- Processing time sensitive data on-premises level while using cloud resources for non-real-time processing tasks.
- Enables us to implement multi-layered security controls which are tailored to specific requirements of industrial environment.
- Enables to detect and respond to security threats more effectively and provides real time security updates and analysis of emerging technologies while on-premises integration enables us to take immediate action to mitigate the risk locally.
- Provides utilization of cloud based centralized monitoring, threat detection while on-premises can offer only localized protection for the critical systems and threats.

Compared to hybrid proposed hybrid approach, traditional IoT security methods, due to increasing number of IoT devices, these approaches are struggling to scale effectively potential security vulnerabilities. Those methods might be less flexible and adaptable where it causes challenges to respond to new security threats and changes in effective way. In addition, in those approaches, there might be lack of redundancy and resilience where those are needed to withstand security breaches and system failures and it leads to potential downtime in the system and data loss. Moreover, from time to time these security solutions may require significant investment in hardware and software maintenance and it leads to higher total cost of the ownership of security of the build system over time.

By considering these advantages, the proposed hybrid approach provides more comprehensive, flexible, and resilient security strategy compared to traditional IoT security mechanisms. By combination of these strengths of both cloud and on-premises, industrial organizations can better protect their IoT devices and data against a wide range of security threats while meeting scalability, compliance and efficiency requirements.

6. Implemented Real World Scenarios

Currently, there are many big industrial companies implementing this hybrid approach in their solutions for the industry. One of the examples that can be shown is Predix platform that is provided by GE [22]. This platform is based on hybrid model to address diverse security requirements for industrial IoT environments. On the cloud level this

platform includes various types of cloud services such as AWS or Azure, identity and access managements systems, data protection and security monitoring.

Another real-time world scenario example could be the utilization of hybrid solution in oil and gas explorations. As, this type of industries is operating remote drilling sites and offshore platforms where these sites are equipped with IoT sensors, cameras, control systems to monitor the deployed equipment performance, detection of the leaks and ensure environmental compliance. Today, those industries are adopting hybrid cloud and on-premises based approaches to secure their IoT ecosystem in challenging remote environments. For protecting the critical infrastructure and operational data at source, on-premises are being deployed. Meanwhile, utilizing cloud-based data analytics, application of machine learning algorithms and implementation of threat detection systems for anomalies, enables infrastructure to have more granular secure ecosystems.

On the other hand, to extend security measures for the edge devices, implementation of on-premises solution is enabling industry to utilize on premises firewalls and intrusion detection systems and secure gateways to protect to local network for the IoT devices. In return, this model provides balanced and flexible solutions for unique challenges of securing iot devices in the industry. By combining this approach, organizations to achieve comprehensive security coverage, resilience, and compliance in the IIoT deployments.

7. Conclusion

In this context, we first classified solutions on how to secure devices by isolating them against physical impacts – namely, the isolation of devices, which this approach makes an obstacle against physical and man-in-the-middle attacks. Further, we investigated the security of devices at the server level, and for this method, we considered an MQTT-enabled on-premises-based server. The reason for choosing this solution is to implement device authentication and access authorization. As a last step, we mainly consider a security approach on the cloud side, especially Azure Cloud. In terms of cloud security, we mainly focus on cloud services, such as IoT Hub, NSGs, Vnets, private endpoints, and authentication methods using Azure Active Directory. As a result, we strongly believe that by taking these given actions, it is possible to ensure IIoT ecosystem security, and it is possible to implement them even in the larger IIoT ecosystem.

References

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

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

[3] 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.

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

[5] 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.

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

[7] Eric D. Knapp and Joel Thomas Langill, "Industrial Network Security (Second Edition)" {Syngress}.,2015.

[8] Omerah Yousuf, Roohie Naaz Mir "A survey on Internet of Things security: State of art, architecture, issues and countermeasures", 2019.

[9] Lubna Luxmi Dhirani, Eddie Armstrong and Thomas Newe, "Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap," {IEEE Wireless Communication and Networking Workshops}.,2021.

[10] Joseph Jose Anthraper, Jaidip Kotak, "Security, Privacy and Forensic Concern of MQTT protocol,"{International Conference on Sustainable Computing in Science}., 2019 DOI:10.2139/ssrn.3355193

[11] MQTT Version 5.0. Edited by Andrew Banks, Ed Briggs, Ken Borgendale, and Rahul Gupta. 07 March 2019. OASIS Standard. https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt v5.0-os.html. (accessed 25.02.2023).

[12] www.upguard.com/blog/network-segmentation-best practices (accessed 09.16.2023). DOI: Not available

[13] 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

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

[15] 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}.,

[16] Microsoft Azure https://learn.microsoft.com/en us/azure/iot-hub/iot-hub-tls-support (accessed 03.03.2023).

[17] Eric D. Knapp and Joel Thomas Langill, "Industrial Network Security (Second Edition)" {Syngress}.,2015.

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

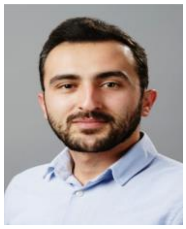
[19] Microsoft Azure https://learn.microsoft.com/en us/azure/virtual-network/ (accessed 01.03.2023).

[20] 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.

[21] [White Paper] The Four Pillars of a Trusted Industrial Information Infrastructure (aveva.com) (accessed 01.05.2024).

[22] GE Predix Platform | Industrial IoT Platform | GE Digital (accessed 01.03.2024).

Author's Profile



Orkhan Aslanli is a researcher at the department of theoretical computer science, data security and cryptography in the faculty of informatics in Hungary, Debrecen, University of Debrecen. His research interests network security of internet of the things and constrained IoT devices.

How to cite this paper: Orkhan Aslanli, "Cloud and On-premises Based Security Solution for Industrial IoT", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.16, No.5, pp. 55-62, 2024. DOI:10.5815/ijieeb.2024.05.02