IoT Cloud Implementation: Cybersecurity Point of View

José Ferreira

Universidade Lusófona, Porto, Portugal info.cul@ulusofona.pt
www.ulusofona.pt

Abstract. For this paper, the focus is a thorough explanation of cybersecurity and its importance to the modern landscape of the Internet of Things (IoT). It begins with the importance of cybersecurity and an overview of the concepts involved, and then it moves to an explanation of what is IoT.
To examine the security of IoT, the study presents an implementation using Azure IoT. This is followed with an exploration of the security features used in this system, including how they work and how effective they are.

Keywords: iot · cybersecurity · hacking · azure iot. · TLS · MQTT · X.509 certificates

1 Introduction

In the contemporary landscape of technology, the convergence of cybersecurity and the Internet of Things (IoT) has emerged as a focal point of exploration and practical implementation. This paper delves into the significance of cybersecurity in the face of evolving cyber threats, and subsequently explores the transformative potential of IoT across various industries.

As we navigate through this discourse, it is crucial to acknowledge the expanding threat landscape that underscores the imperative for robust cybersecurity measures. In a world where digital vulnerabilities are exploited with increasing sophistication, the need to fortify our digital infrastructure becomes not just a consideration but a critical mandate.

Transitioning from this acknowledgement, our exploration extends into the realm of the Internet of Things—a technological evolution where everyday objects are imbued with sensors, software, and connectivity. This paradigm shift in data collection and utilization has far-reaching implications, evident in the transformative impact of IoT across diverse sectors, from manufacturing to people's homes.

To ground our theoretical examination, the paper turns its attention to a practical implementation—an IoT system designed for a small garden, integrated into the Azure ecosystem. This application serves as a demonstration of Azure in supporting IoT solutions and examination of the intricacies of cybersecurity within a real-world technological framework.

The paper concludes with a dissection of the security features embedded in this system, ranging from the nuances of the MQTT protocol to the robust layers of security provided by Transport Layer Security (TLS) and X.509 certificates.

2 Cybersecurity: a brief explanation

2.1 Cybersecurity

Cybersecurity as defined by Microsoft [3] and IBM [2] is any practice, technology, measure or process that intends to protect individuals organizations from cybernetic attacks

A Cyberattack is any deliberate attempt to gain unauthorized access to a network, computer system, or digital device in order to steal, expose, alter, disable, or destroy data, applications, or other assets.[1]

A Vulnerability needs to exist before an attack can exploit it. It can be defined as an existing weakness inside a system, procedure, controls or implementation that can be used by an attacker [7]

The importance of cybersecurity Understanding the scope, application, and appropriate usage of cybersecurity is crucial. As many people mistakenly believe, cybersecurity is not just about protecting computers online. To protect the hardware, software, data, and information found in an online system (the internet) against any type of compromise is to practice cybersecurity.

Nowadays, cybersecurity extends to include protecting electronic equipment and devices (Internet of Things) against illegal use, changing projections. Data protection and information security are given top importance for organizations when implementing cybersecurity, whilst privacy and access control are given priority for people. Using cutting-edge machine learning techniques, cybersecurity is currently used to protect people from cyberbullying and detect cyberwarfare. [6]

Businesses can be disrupted, damaged, or destroyed by cyberattacks, and the cost to victims keeps going exponentially. For instance, the Cost of a Data Breach 2023 report from IBM states that [1]

- In 2023, the average cost of a data breach was 4.1 million Euros, a 15% increase over the previous two years;
- In 2023, a ransomware-related data breach cost an average of 4.7 million euros, which was significantly higher. This excludes the price of the ransom, which increased by 89 percent from the prior year and averaged an additional 1.4 million euros.

The rise in cloud computing adoption, network complexity, remote work programs, bring your own device (BYOD) policies, and IoT are just a few of the information technology (IT) trends of the last few years. While these trends have greatly benefited businesses and advanced humankind, they have also exponentially increased the number of attack vectors available to cybercriminals.

Main types of cybersecurity threats

Phishing is a method of social engineering that involves sending emails, texts, or voicemails that seem to be from a trustworthy source in order to persuade recipients to divulge personal information or click on an unknown link. In a phishing campaign, a large number of e-mails are sent to a large number of people in the hopes that one of them will click the link. Some operations, known as spear phishing, are more individualized and person-specific. For instance, an attacker might pose as a jobseeker to deceive a recruiter into downloading a résumé that is contaminated.

Social engineering is when attackers trick victims into giving up account information or downloading malware by playing on their trust. In these attacks, criminals assume the identity of a well-known company, colleague, or friend and employ psychological tricks such invoking a sense of urgency to influence victims into acting in accordance with their wishes.

Malware is any malicious software, including viruses, worms, ransomware, and spyware. By changing or destroying files, extracting private information like passwords and account numbers, or by sending nefarious emails or traffic, it is intended to harm systems or networks. Malware can be installed by an attacker who has gained access to the network, unintentionally by a victim of phishing.

Ransomware is software that encrypts files and renders them unavailable. It is a type of extortion. During a ransomware assault, the attackers often steal data and may threaten to make it public if they are not paid. Victims are required to pay a ransom in exchange for a decryption key.

Insider threats are actors who are legally inside the network or system and cause a breach in security. These actions may be intentional or accidental. [3]

3 IoT: A brief explanation

The Internet of Things (IoT) according to companies in the vanguard of this, technology [4] [5], is a network of physical objects, including machines, cars, appliances, and other items, that have sensors, software, and network connectivity built into them to enable data collection and sharing. These items, commonly referred to as "smart objects," might include everything from straightforward "smart home" gadgets like smart thermostats to wearables like smartwatches and RFID-enabled clothes to sophisticated industrial machinery and transportation systems.

IoT connects common "things" to the web. Engineers have been incorporating sensors and CPUs into commonplace items since the 90s. However, the technology was large and cumbersome, progress was first slow and confined to industrial environments. RFID tags, which are small, low-power computer chips, were initially employed to track expensive machinery. These processors evolved over time to become smaller, quicker, and smarter as computer devices shrunk in size [4].

IoT has a wide range of possible applications, and its effects are already being seen in a number of different sectors, including manufacturing, transportation, healthcare, and agriculture. IoT is set to play an increasingly significant role in reshaping our world and altering how we live, work, and interact with one another as the number of internet-connected devices increases [5].

Architecture of IoT can only be defined in a generic model, as the major players in IoT are not in agreement of a uniform, standardized reference model.

Frustaci et al. [8] argue that 3 layers can fully describe an IoT system: Perception, Transportation and Application

The system starts in the perception layer, It is the one containing all the components that collect data and process it.

The second layer, transportation, gives access to the first layer in order to pass the received information to any system that will process it. The information is carried through available local networks or the internet.

The last layer, application, is the one responsible for providing to users the services they request. This is where the services for enterprises and cloud computing systems are supported.

4 An implementation of IoT using Azure

For the purposes of this paper, an IoT system was designed for a small garden connected to a house. The system allows the owner to monitor the temperature, humidity and light intensity in two points of the garden. These IoT sensors are powered by batteries charged by solar power, with a small solar panel for each trio of sensors. Near the house, there is a controller for the irrigation system. They are connected to the internet by a Wi-Fi repeater set up in the same place as the controller. All devices are programmed using Azure IoT device Python SDK's (Software development Kit). This garden setup is shown in Figure 1

The Cloud part of the implementation is shown in Figure 2. The devices communicate with the cloud through Wi-Fi using the MQTT (Message Queuing Telemetry Transport) protocol, a protocol that's very lightweight, secure and ideal for small devices [13]. Azure IoT Hub is responsible for routing all messages coming and going to the devices. The data from the messages is analyzed by Azure Stream Analytics, a real-time analytics service that can process the incoming data and send the resulting processed data to Azure IoT Central, who provides the interface for the user on their mobile device or computer.

Stream Analytics will, when the data describes certain scenarios, like a drop below a certain temperature, generate an alert. This alert can be sent to the user interface and/or to the final component, Azure Functions, as an event trigger. This Event trigger can also be sent manually by the user. Azure Functions will then send an order, through the hub, to the devices, for example to turn on the irrigation system.

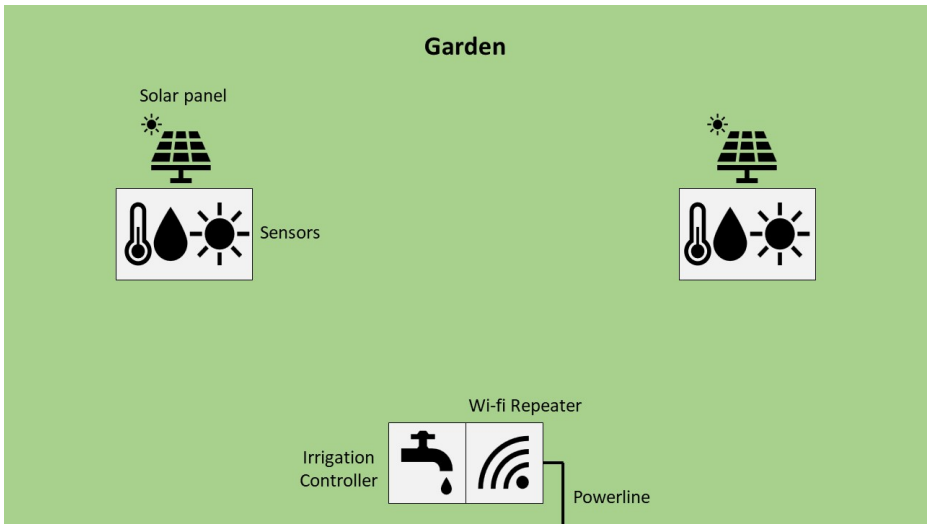

Fig. 1. Garden IoT system.[22]

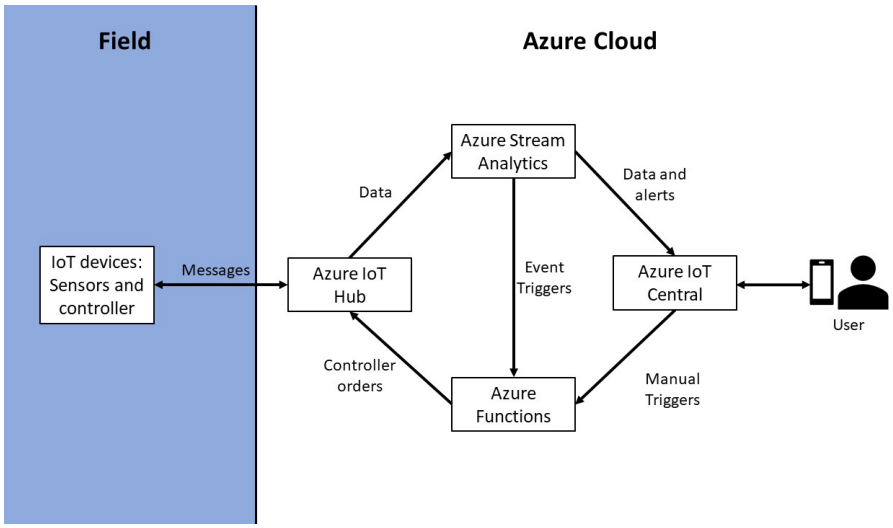

Fig. 2. Azure implementation in the Garden IoT system.[23]

In terms of security features and protocols, we are using the Device Provisioning Service (DPS) to register the IoT devices with the IoT Hub. This service allows us to securely attest our IoT devices with X.509 certificates to ensure the identity of each device and assign it to our IoT Hub [12]. This and other protocols and features will be explored in the next chapter.

5 Security features

In this chapter, we will look at features used in the system we have described in the previous chapter and find if they are secure, if they are not, we will look and what can be done to make them secure. We will start with a protocol already mentioned in that chapter, MQTT protocol, and from there we will move other features that provide more robust security to that protocol.

MQTT (Message Queuing Telemetry Transport) Protocol MQTT is, as described by MQTT.org [13] and Amazon [14], a standards-based messaging protocol that allows for efficient transmission of data in IoT devices that constrained resource-wise, such as the sensors used in our garden IoT system. It also permits low bandwidth usage [15]. The principle used in the MQTT protocol is a publish/subscribe model with topics using a message broker to take care of the communication between the publisher and the subscriber, decoupling senders from receivers.

In our implementation, Azure IoT Hub acts as the broker and entry point to the cloud. The devices can publish to topics such as *sensor/reading* to transmit for example the current temperature read by a sensor, and they can subscribe to topics to receive data or instructions such as the command to start the irrigation. This is described in Figure 3.

However, Microsoft [16] warns that IoT Hub isn't a full-featured MQTT broker and doesn't support all the behaviors specified in the MQTT v3.1.1 standard. We are limited to 256-kb maximum message size and have no support for device-to-device communication. As the data provided by our devices is very simple, involving only one value per sensor and the irrigation system receives simple start/stop orders with no direct communication between devices, this limitations work in our favor as they also limit what bad actors can do if they gain access to the system.

Microsoft also states that the use of TLS/SSL is obligatory for communications using IoT Hub, the necessity for this transport layer is backed by literature [15] declaring that information carried by MQTT is easily accessed if the protocol is used without TLS or any other defenses.

TLS (Transport Layer Security) TLS is a widely used security protocol that provides privacy and data security in communications over the internet. Introduced in 1999 and in its current version, 1.3, since 2018, it ensures that transmitted data is hidden from unintended observers, that it is not tampered

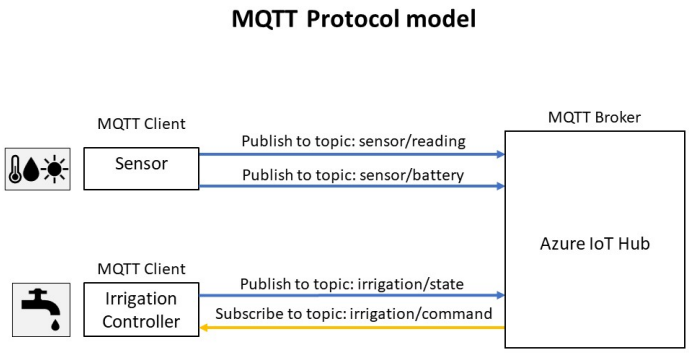

Fig. 3. MQTT Protocol model in the Garden IoT system.[24]

and ensures the authentication of sender and receiver. It is also known as SSL, as it was the name of the protocol that TLS has succeeded [17].

It achieves this with a process called handshake, during which the sender and the receiver decide which version of TLS and which cipher suite they will use and use the TLS certificates to verify their identities. After the handshake, the message is encrypted with keys generated for the session. Finally, the message is signed with an authentication code (MAC) that guarantees its integrity [17].

Besides being required by azure IoT, Ahmad et al. [15] state that TLS in conjunction with MQTT enhances security and provides confidentiality for communications and should be used, even though they warn that the protocol is computationally heavier and uses more bandwidth, as backed by other studies [18], so the frequency of data refreshing in the IoT system might have to be decreased to save resources or instead more resourceful devices will have to be chosen. Alkhafajee et al. [18], in the case of TLS not being possible with the device's resources, offer the alternative of encrypting the *publish* messages and the client's *connect* message with TLS-PSK cipher suite.

X.509 Certificates X.509 Certificates are digital certificates that conform to the IEFT's RFC 5280 standard and can be used to secure network communications in protocols such as HTTPS and TLS by verifying that a public key really belongs to the identity in the certificate. This is accomplished with the X.509 public key infrastructure (PKI) [19] [20].

These certificates need to be issued by a trusted by a trusted third party, a certificate authority (CA). The CA accomplish this by signing the certificates with a private key, while the public key is made available so that systems or

users can verify the signature. X.509 certificates have the capability to sign other certificates. This is important for the public key infrastructure because it creates a chain of trust (a certificate chain), which means the devices don't need to contact the certificate authority when they use certificates [19] [20].

Azure IoT Hub allows the use of X.509 certificates by uploading the certificate authority certificate and proving ownership of the private key. This will make it harder for any attacker to impersonate a device and send false information or malicious commands to the system [19].

The X.509 certificates can also be used in encryption with the public key, allowing only entities with the private key to read the encrypted data [19] [21].

Literature [21] confirms that the process of authentication is the most important safety measure to reduce hacker attacks, and X.509 certificates undeniably make systems more protected.

6 Conclusion

In conclusion, this exploration into cybersecurity, IoT, and an implementation of an Azure-supported garden system provides valuable insights and implications.

Firstly, the significance of cybersecurity is underscored by the escalating threat landscape. The exponential increase in the cost of cyberattacks accentuates the critical need for robust cybersecurity measures to safeguard businesses and individuals from potential disruption and damage.

Secondly, the transformative influence of the Internet of Things is evident in its diverse applications across manufacturing, transportation, healthcare, and agriculture. The system's adaptability and potential to reshape various sectors highlight the far-reaching impact of IoT.

Thirdly, the implementation of an IoT system within the Azure framework demonstrates the platform's capabilities. The integration of solar-powered sensors, coupled with cloud-based decision-making, exemplifies Azure's role in the realization of IoT solutions.

Lastly, the analysis of security features reveals an effective defense strategy. Despite the limitations of the MQTT protocol within Azure IoT Hub, its alignment with the system's requirements is evident. The mandatory utilization of Transport Layer Security (TLS) ensures encrypted and secure communication, while X.509 certificates enhance identity verification, encryption, and overall system integrity.

In the context of cybersecurity and IoT, meticulous attention to security measures is paramount. This conclusion affirms the security of the garden IoT system, emphasizing the security and usefulness of the Azure ecosystem.

References

1. IBM. *What is a cyberattack?* https://www.ibm.com/topics/cyber-attack. Accessed on 14th October 2023.

2. IBM. *What is Cybersecurity?* https://www.ibm.com/topics/cybersecurity. Accessed on 12th October 2023.
3. Microsoft Security. *What Is Cybersecurity?* https://www.microsoft.com/en-us/security/business/security-101/what-is-cybersecurity. Accessed on 12th October 2023.
4. Amazon Web Services, Inc. *What is IoT? - Internet of Things Explained - AWS* https://aws.amazon.com/what-is/iot/. Accessed on 8th October 2023.
5. IBM. *What is the internet of things?* https://www.ibm.com/topics/internet-of-things. Accessed on 8th October 2023.
6. S. S. Tirumala, Maheswara Rao Valluri, GA Babu. *A survey on cybersecurity awareness concerns, practices and conceptual measures.* In: 2019 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-6, 2019. https://doi.org/10.1109/ICCCI.2019.8821951
7. Branko Bokan, Joost Santos. *Managing Cybersecurity Risk Using Threat Based Methodology for Evaluation of Cybersecurity Architectures.* In: 2021 Systems and Information Engineering Design Symposium (SIEDS), pp. 1-6, 2021. https://doi.org/10.1109/SIEDS52267.2021.9483736
8. Mario Frustaci, Pasquale Pace, Gianluca Aloi, Giancarlo Fortino. *Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483-2495, 2018. https://doi.org/10.1109/JIOT.2017.2767291
9. Microsoft. *What is Azure Internet of Things (IoT)* https://learn.microsoft.com/en-us/azure/iot/iot-introduction. Accessed on 11th November 2023.
10. Aina'u Shehu Muhammed, Derya Ucuz. *Comparison of the IoT Platform Vendors, Microsoft Azure, Amazon Web Services, and Google Cloud, from Users' Perspectives.* In: 2020 8th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-4, 2020. https://doi.org/10.1109/ISDFS49300.2020.9116254
11. Microsoft. *Azure IoT reference architecture* https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/iot. Accessed on 12th November 2023.
12. Microsoft. *What is Azure IoT Hub Device Provisioning Service?* https://learn.microsoft.com/en-us/azure/iot-dps/about-iot-dps. Accessed on 25th November 2023.
13. MQTT.org. *MQTT: The Standard for IoT Messaging* https://mqtt.org/. Accessed on 26th November 2023.
14. Amazon AWS. *What is MQTT?* https://aws.amazon.com/what-is/mqtt. Accessed on 26th November 2023.
15. M. Z. Ahmad, A. R. Adenan, M. S. Rohmad, Y. M. Yussoff. *Performance Analysis of Secure MQTT Communication Protocol. 2019 19th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*, Kedah, Malaysia, 2019, pp. 225-229. https://doi.org/10.1109/CSPA57446.2023.10087603.
16. Microsoft. *Communicate with an IoT hub using the MQTT protocol* https://learn.microsoft.com/en-us/azure/iot/iot-mqtt-connect-to-iot-hub. Accessed on 26th November 2023.
17. Cloudflare. *What is TLS (Transport Layer Security)?* https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/. Accessed on 26th November 2023.
18. A. R. Alkhafajee, A. M. A. Al-Muqarm, A. H. Alwan, Z. R. Mohammed. *Security and Performance Analysis of MQTT Protocol with TLS in IoT*

Networks. 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), Najaf, Iraq, 2021, pp. 206-211. https://doi.org/10.1109/IICETA51758.2021.9717495.
19. Microsoft. *Authenticate identities with X.509 certificates* https://learn.microsoft.com/en-us/azure/iot-hub/authenticate-authorize-x509. Accessed on 26th November 2023.
20. A. Alrawais, A. Alhothaily, X. Cheng. *X.509 Check: A Tool to Check the Safety and Security of Digital Certificates. 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)*, Beijing, China, 2015, pp. 130-133. https://doi.org/10.1109/IIKI.2015.36.
21. S. Karthikeyan, T. Poongodi. *Secured Data Compression and Data Authentication in Internet of Thing Networks Using LZW Compression Based X.509 Certification. 2022 IEEE International Conference on Data Science and Information System (ICDSIS)*, Hassan, India, 2022, pp. 1-5. https://doi.org/10.1109/ICDSIS55133.2022.9915855.
22. Ferreira, José. *Garden IoT system.* 2023.
23. Ferreira, José. *Azure implementation in the Garden IoT system.* 2023.
24. Ferreira, José. *MQTT Protocol model in the Garden IoT system.* 2023.