Security aspects in the Agriculture IoT infrastructure: Network segmentation and security infrastructure perimeter*

Pavel Ambruz[1,*,†], Vladimír Voral[1,†], Michal Stočes[1,†] and Jiří Vaněk[1,†]

[1] *Czech University of Life Sciences Prague, Faculty of Economics and Management, Kamýcká 129, 16500 Praha-Suchdol, Czechia*

Abstract

This thesis focuses on the analysis of security aspects within the Internet of Things (IoT) infrastructure, specifically targeting endpoint unmanaged devices. Security issues within the IoT infrastructure are intricate, presenting a broad spectrum of potential challenges that can be addressed or optimized. In this domain, the fundamental elements constitute an integral part of the overall infrastructure security. The study examines the issue of inadequate communication security from endpoint devices, which requires detailed exploration and an effort to define universal security standards. The primary challenge lies in the design of the infrastructure and the implementation of network segmentation, which was successfully identified.

Keywords

Internet of Things (IoT), security, network segmentation, endpoint devices, infrastructure, communication

1. Introduction

In the context of the Internet of Things (IoT) [1], it is essential to note that although this technology brings significant advantages in terms of simplicity and efficiency, many individuals neglect the security aspects associated with this specific network domain [2]. In today's modern world full of automation and robotization, it is entirely unthinkable to do everything manually, and sometimes people overlook fundamental building blocks. In many instances, IoT networks have become the primary target of cyber-attacks, primarily due to inadequate security measures.

In the agricultural sector, IoT devices are ubiquitous, ranging from common automatic irrigation systems to sensors monitoring the quality of plant growth. This network is extensive, and management and maintenance are demanding [3]. The aim of this work is to define basic security elements of the infrastructure, including network segmentation and communication with end devices within the agricultural IoT infrastructure.

2. Current state of the art

In recent years, the agricultural sector has undergone significant transformation due to the integration of Information and Communication Technology (ICT) and the Internet of Things (IoT). The rising global demand for increased productivity and efficiency, coupled with the necessity to

* *Short Paper Proceedings, Volume I of the 11th International Conference on Information and Communication Technologies in Agriculture, Food & Environment (HAICTA 2024), Karlovasi, Samos, Greece, 17-20 October 2024.*

* Corresponding author.

† These authors contributed equally.

ambruzp@pef.czu.cz (P. Ambruz); voral@pef.czu.cz (V. Voral); stoces@pef.czu.cz (M. Stočes); vanek@pef.czu.cz (J. Vaněk)

0009-0001-6234-0620 (P. Ambruz); 0009-0009-3195-189X (V. Voral); 0000-0001-7128-1071 (M. Stočes); 0000-0002-4573-5348 (J. Vaněk)

reduce costs and optimize labor utilization, has propelled ICT and IoT solutions to the forefront, garnering substantial interest from farmers and agricultural enterprises. The incorporation of IoT technologies into agriculture has led to the emergence of numerous impactful applications, including precise analysis of crop productivity, real-time monitoring of crop health, soil nutrition management, rainfall tracking, water management, and pest infestation monitoring. Various IoT systems and applications, such as decision support tools, automated irrigation systems, frost protection mechanisms, remote monitoring platforms, and precision fertilization systems, exemplify the practical implementation of IoT technology within the agricultural sector. This shift towards a technology-driven approach in agriculture is often referred to as Precision Farming or Precision Agriculture. According to Wolf and Wood, Precision Farming utilizes technologies like the Global Positioning System and digital agricultural measurements to enhance the precision and efficiency of crop production, particularly in areas such as fertilizer application, pest control, and water conservation. This is a new era of efficiency, productivity, and sustainability in farming practices on a global scale [8].

2.1. Infrastructure of IoT

People generally tend to understand the Internet of Things as a group of connected devices. This is vital knowledge from an IoT infrastructure standpoint, as the user will determine the elements you need to include in your support system. As such, you need to consider that the IoT is broken down into 2 core types: consumer and industrial. There are two core types of IoT infrastructure: Consumer IoT (CIoT) and industrial IoT (IIoT). The first type is consumer IoT, where the devices in this particular ecosystem are usually focused on providing convenience and quality-of-life improvements for individual private users. This often includes consumer gadgets like smart refrigerators, smart lighting systems, and wearable technology. The CIoT also tends to be less data-heavy, although this can vary from user to user. While the CIoT is still subject to security risks, the scope for disruption also tends to be relatively limited. The second type is industrial IoT, which is more commonly termed IIoT. The intention of the IIoT tends to be centered on improving the efficiency and efficacy of business operations. These devices are designed to capture, analyze, and interpret industrial intelligence, so business leaders can make real-time process adjustments. Increasingly, the IIoT is adopted to support safety in the workplace [13].

2.2. IoT endpoints

The Internet of Things (IoT) constitutes a vast network of interconnected devices that are equipped with sensors, software, or other technologies enabling them to gather, store, and exchange data through the internet.

Within the realm of IoT, the spectrum of devices is extensive and diverse. It encompasses not only traditional endpoints such as computers, laptops, mobile phones, tablets, and servers but also extends to encompass a plethora of non-traditional items. These include printers, cameras, household appliances, smartwatches, health trackers, navigation systems, smart locks, and intelligent thermostats, among others [9].

The primary objective of research related to Precision Agriculture is to develop a comprehensive Decision Support System (DSS) for farm management, aimed at optimizing outcomes while minimizing inputs and conserving resources. Precision Agriculture leverages a wide array of IoT devices and electronic sensors for monitoring and controlling production processes. Traditionally, agriculture was predominantly viewed as a heavily mechanized and offline industry. Increasingly, farms are interconnecting their systems to enable remote access, facilitating seamless monitoring and control. As emphasized, Precision Agriculture relies on digital technologies to achieve its objectives. According to the European Commission, the most prevalent technologies in Precision Agriculture include object identification, georeferencing, measurement of physical and chemical parameters, satellite navigation, connectivity, data storage and analysis, process automation, and vehicle guidance. This evolution signifies a departure from conventional agricultural practices

towards a more digitally integrated and data-driven approach, with the overarching goal of enhancing efficiency and sustainability in farming operations [12].

2.3. Network segmentation

Network segmentation involves breaking down a computer network into smaller segments. This approach aims to enhance both the performance and security of the network. It's often referred to using synonymous terms such as network segregation, network partitioning, and network isolation [11].

Network segmentation is another integral component in infrastructure design, without which it is no longer possible to proceed in today's context. To best implement communication rules through the firewall, it is necessary to divide the individual parts of the network into segments to which routing rules will be assigned.

Segmentation offers advantages from several straightforward aspects, including easier implementation of rules, microsegmentation, clearer communication and querying of end devices, and last but not least, from a security perspective.

3. Secure IoT infrastructure

To designate infrastructure as secure, it is essential to build it in accordance with security standards and ideally test it against basic cyber-attacks. During the design phase of the infrastructure, it is also necessary to consider several aspects that will affect overall security [14]. Therefore, first, the types of end devices to be used in the infrastructure and with whom they will communicate are defined. Subsequently, a network infrastructure protected by a firewall is prepared. This simple approach results in the creation of a standard secure infrastructure.

Steps to building a secure IoT infrastructure:

- Definition of the type and nature of connections of end devices
- Determination of the scope of IoT devices in the planned network
- Creation of segmentation based on the previous points

Implementation of a firewall and rules corresponding to the previous steps

3.1. Security problem with endpoints

The key element in the infrastructure is the endpoint device, without which it would not make sense to build the entire infrastructure, and it is also the most problematic part [4]. Smart devices, which constitute a significant subset of endpoint devices, can be divided into manageable and unmanageable categories, as not every device requires an operating system for its functionality. In cases where an operating system is implemented in the device, securing communication to the network is much easier than with ordinary sensors [5].

This seemingly negligible error is the cause of the most common cyber-attack known as "man in the middle" [6]. Unmanaged devices continue to transmit signals that can be altered by the attacker, and based on these instructions, they can cause a catastrophic system failure, such as improper irrigation system control, leading to flooding of the entire plantation.

The issue is addressed already during the design phase of integrating end devices into the network. At this point, it is crucial to understand how the given device operates and how to best integrate it into the network. There are two connection options: using a cable, which is considered secure in terms of "man-in-the-middle" attacks or using Wi-Fi. In both cases, it is essential to ensure the authorization of the end device and its proper inclusion in the communication segment. For radio connections, establishing authorization for the end device is even more critical to prevent signal tampering.

3.2. The robustness of agricultural IoT infrastructure

In network infrastructures, such as in the agricultural sector, the network may consist of several thousand end devices that need to communicate with each other. It is necessary to consider the size and potential scalability or reduction of the network, as this infrastructure is highly dynamic. In large and robust networks, security is implemented by dividing the network into areas that communicate with each other, and network segmentation is performed within these areas [16].

Within the network, an area containing several greenhouses may be defined, which are further segmented and protected by security rules. Another area of agricultural infrastructure may be the irrigation system across different fields. Each of these areas is secured by a firewall at its perimeter, which regulates communication with other areas based on rules. Only through this approach can clarity and secure communication across the entire infrastructure be ensured.

3.3. The importance of network segmentation

IoT devices, located in a different network segment than the end user, are protected against potential cyber-attacks from the user [7]. From this fact, it follows that segmentation must be included in the initial infrastructure design, as access to the IoT network segment will be granted only to the administrator or operator of these devices.

At first glance, network segmentation may seem easy, but it is necessary to consider that the IoT infrastructure of a single greenhouse can be extensive. The first step is to divide the end devices into several segments and determine their priority in the network. The ideal solution for network segmentation is to divide end devices according to their functionality and importance.

- Managed devices (equipped with an operating system)
- Unmanaged devices (without an operating system)
- Active network components (switch, router, firewall)
- User stations
- Administrative stations
- Data storage

3.4. Implementation of secure rules and firewall

For the proper implementation of routing security policies into the network, it is essential to establish network segmentation, as defined in the previous chapter. Based on clearly defined segmentation, routing rules can be implemented to ensure that only the correct devices access the network. Taking, for example, the IoT greenhouse infrastructure [17], it is crucial that only connections from the network administrator, data storage for sensor data collection, and monitoring applications that control the entire automation system are allowed into this network. The routing rules configuration is presented in Table 1.

Table 1
Routing rulers for secure IoT infrastructure in the greenhouse

	IoT devices	Administrator	Monitoring center	Data storage	Users
IoT devices	permit	permit	permit	permit	deny
Administrator	permit	permit	permit	permit	permit
Monitoring center	permit	permit	permit	deny	deny
Data storage	permit	permit	deny	permit	deny
Users	deny	permit	deny	deny	permit

In this implementation of routing rules into network segmentation, it is not possible for any user to communicate with the IoT structure, and this simple design excludes attacks from the user network [7]. The correct procedure for the administrator is for the user station to connect to a virtual administrative station; this network passage is illustrated in Table 1. Subsequently, the virtual administrative station can communicate with other network segments. This infrastructure concept can be termed secure, and in the event of any attack, it is clearly identifiable from which segment the attack originates. The most suitable device for implementing routing rules is a firewall, which not only directs data traffic in the network but also logs rule violations and can generate alerts [15], which are highly beneficial for the monitoring center, enabling it to quickly and effectively respond to cyber incidents in the entire proposed secure agricultural IoT infrastructure.

4. Discussion

Our proposal for secure agricultural IoT infrastructure focuses on the primary network design, segmentation, and endpoint devices. Most other security proposals deal with data encryption transmitted across the network or design detection mechanisms for cyber-attacks using artificial intelligence to prevent attacks in real-time. According to published results, all these proposals are relatively functional and provide a very high level of infrastructure security.

Our intention was to create a security concept that would serve as a general framework for building a secure IoT infrastructure. It is important to note that most IoT devices are unmanageable, and implementing encryption or other software mechanisms into them is essentially impossible. Therefore, it is crucial to focus on designing the entire infrastructure and properly dividing the network functions into segments that will communicate with each other based on security rules.

It is true that implementing detection mechanisms using artificial intelligence is likely easier than re-evaluating the entire infrastructure concept, but it is necessary to consider the objectives and the amount of time and resources it will require. An important factor is that even in the case of software implementation into the infrastructure, it is necessary to understand the entire network topology, its functions, and requirements for smooth operation. This step marks the beginning of our secure infrastructure variant, as without the right input data, security measures cannot be implemented.

5. Conclusions

The present variant of secure agricultural IoT infrastructure requires a more comprehensive understanding of the entire network, yet it leads to a much clearer infrastructure on which all security measures can be better and more accurately applied. This study also aims to assist existing extensive IoT networks, as even basic network segmentation deployment leads to a rapid increase in infrastructure security. The entire proposal needs to be thoroughly tested, particularly regarding endpoint smart devices, where many additional questions arise regarding device authorization into the network and management of encryption keys. All these individual aspects will be examined in the forthcoming publications.

Acknowledgements

This work was supported by the EC's Horizon Europe funding in the project CODECS, grant no. 101060179.

The results and knowledge included herein have been obtained owing to support from the following institutional grant. Internal grant agency of the Faculty of Economics and Management, Czech University of Life Sciences Prague, grant no. IGA 2023B0005.

This research was carried out under the project: "Precizní zemědělství a digitalizace v ČR" (Precision Agriculture and Digitalization in Czech Republic), reg. no. QK23020058.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] Bonaventure, O. (2011) 'Computer Networking : Principles, Protocols and Practice'. Available at: http://dlib.hust.edu.vn/handle/HUST/22916 (Accessed: 24 April 2024).

[2] Lamaazi, H. *et al.* (2014) 'Challenges of the Internet of Things: IPv6 and Network Management', in *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 328–333. Available at: https://doi.org/10.1109/IMIS.2014.43.

[3] Elijah, O. *et al.* (2018) 'An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges', *IEEE Internet of Things Journal*, 5(5), pp. 3758–3773. Available at: https://doi.org/10.1109/JIOT.2018.2844296.

[4] Zanella, A. *et al.* (2014) 'Internet of Things for Smart Cities', *IEEE Internet of Things Journal*, 1(1), pp. 22–32. Available at: https://doi.org/10.1109/JIOT.2014.2306328.

[5] Yoo, S.J. (2018) 'Study on Improving Endpoint Security Technology', *Convergence Security Journal*, 18(3), pp. 19–25.

[6] Mallik, A. (2019) 'MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS', *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, 2(2), pp. 109–134. Available at: https://doi.org/10.22373/cj.v2i2.3453.

[7] Assistant Professor, Department of Management Studies, University of Kashmir, India *et al.* (2023) 'Stout Implementation of Firewall and Network Segmentation for Securing IoT Devices', *Indian Journal Of Science And Technology*, 16(33), pp. 2609–2621. Available at: https://doi.org/10.17485/IJST/v16i33.1262.

[8] Gómez-Chabla, R.; Real-Avilés, K.; Morán, C.; Grijalva, P.; Recalde, T. IoT applications in Agriculture: A systematic literature review. In ICT for Agriculture and Environment; Valencia-García, R., Alcaraz-Mármol, G., del Cioppo-Morstadt, J., Vera-Lucio, N., Bucaram-Leverone, M., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 68–76

[9] Roeckl, 2022. What is internet of things (IOT) security? URL: https://www.crowdstrike.com/cybersecurity-101/internet-of-things-iot-security/

[10] Dashlane, 2024. What is Network Segmentation & How Does It Work? URL: https://www.dashlane.com/blog/what-is-network-segmentation

[11] Cisco, What Is Network Segmentation?, 2024 URL: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

[12] Trivelli, L., Apicella, A., Chiarello, F., Rana, R., Fantoni, G. and Tarabella, A. (2019), "From precision agriculture to Industry 4.0: Unveiling technological connections in the agrifood sector", British Food Journal, Vol. 121 No. 8, pp. 1730-1743. https://doi.org/10.1108/BFJ-11-2018-0747

[13] Stočes, M.; Vaněk, J.; Masner, J.; Pavlík, J. Internet of Things (IoT) in agriculture—Selected aspects. Agris on-Line Pap. Econ. Inform. 2016, 83–88 at: https://ageconsearch.umn.edu/record/233969/?v=pdf

[14] Wong, A. and Yeung, A. (2009) Network Infrastructure Security. Springer Science & Business Media.

[15] Mhaskar, N., Alabbad, M. and Khedri, R. (2021) 'A Formal Approach to Network Segmentation', Computers & Security, 103, p. 102162. Available at: https://doi.org/10.1016/j.cose.2020.102162.

[16] Tzounis, A. et al. (2017) 'Internet of Things in agriculture, recent advances and future challenges', Biosystems Engineering, 164, pp. 31–48. Available at: https://doi.org/10.1016/j.biosystemseng.2017.09.007.

[17] Novák, V.; Stočes, M.; Čížková, T.; Jarolímek, J.; Kánská, E. Experimental Evaluation of the Availability of LoRaWAN Frequency Channels in the Czech Republic. Sensors 2021, 21, 940. https://doi.org/10.3390/s21030940