Interdisciplinary Description of Complex Systems 21(2), 141-147, 2023

CYBER SECURITY ANALYSIS OF SMART BUILDINGS FROM A CYBER SECURITY ARCHITECTURE POINT OF VIEW

Barnabás Sándor* and Zoltán Rajnai

Óbuda University, Doctoral School on Safety and Security Science
Budapest, Hungary

DOI: 10.7906/indecs.21.2.2
Regular article

Received: 16 September 2022.
Accepted: 15 November 2022.

ABSTRACT

Nowadays, the smart city concept is gaining ground worldwide, driven by the development of information technology and IoT devices. As a result, smart buildings are built to provide more efficient, environmentally friendly, comfortable and automated features. The industry of building automation dates back nearly a hundred years. However, with the development of information technology, the size of built-in IT devices is shrinking year by year, and the amount of information generated by individual sensors, IT devices and by the people working in these buildings is fast increasing. Consequently, IT systems in intelligent buildings need to be adequately designed considering several aspects. Cyber security is one of these aspects, and it is the subject of the present research. A poorly designed and protected IT system with many Internet of Things elements creates a massive exposure to cyberattacks and hackers. After all, these systems may include the entire network IT structure, the elevator control and access control systems, the building's HVAC system, or even the parking lot system. In summary, the examination of primary cyber security factors and standards should be considered when designing a smart building.

KEY WORDS

smart city, smart building, building automation, internet of things, cyber security

CLASSIFICATION

ACM: C.2.1, H.1.1, H.5.1, H.5.3

JEL: L86

*Corresponding author, η: sandor.barnabas@uni-obuda.hu; +;
Népszínház street 8, Budapest, 1081, Hungary

INTRODUCTION

Today, smart cities are not just a concept emerging in research papers and references. They are also gaining ground in practice, as an increasing number of cities worldwide realize that information and communication technologies (ICTs), including Internet of Things (IoT) tools are now becoming the mainstays of infrastructure. A settlement or group of settlements is a smart city if it develops its constructed environment and digital infrastructure, as well as the quality and economic productivity of its services sustainably, with the increased involvement of its inhabitants, using modern and renewable information technologies [1]. One of the distinctive forms of technologies and resources in smart cities is smart buildings, which aim to operate in an environmentally conscious, energy-efficient and economical way and increase the workers' comfort and convenience, thus increasing work efficiency. These buildings are also complex IT and cyber security solutions, including tens of thousands of sensors, actuators, IoT devices, security systems, access control systems, meeting room booking applications, elevators, and, for example, smart gardening systems. These systems, together or individually, can be threatened by cybercriminals, who, for a profit (economic or competitive), sabotage, or other reasons, attack these building systems, causing severe material, intellectual, or life-threatening damage. That is why the IT systems of these buildings must be adequately designed, implemented, and tested for cyber security to prevent or at least reduce such damage. The plans will be developed, modified, and validated by cybersecurity architects, engineers, and field specialists, and they will be deployed by integrator companies as well as tested by vulnerability experts.

WHAT IS A SMART BUILDING?

At first, it might be thought that building automation is an invention of the 21st century, but in fact it dates back more than 100 years. In 1921, the world's first lighting automation was completed, which operated in a staircase in Stuttgart and was made by the Theben company [2]. Automation has evolved steadily over the past 100 years, and convenience features have been added to each mechanical area, such as cooling-heating, fire protection, physical security, building operation, and metering, as shown in Figure 1. The primary purpose of smart buildings is to make connection between the data generated, the people inside, and the various systems [3]. The systems based on different IT solutions are managed centrally and on a cloud basis, making them more efficient to operate and troubleshoot, but more vulnerable to various hacker attacks if they are not adequately controlled on the network.

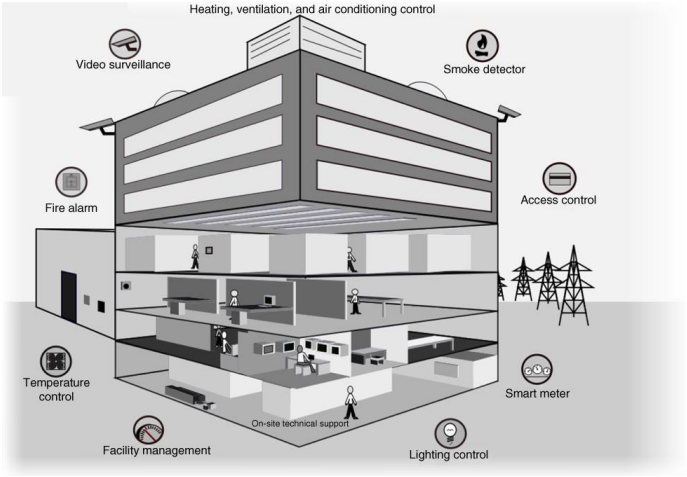

Figure 1. Smart Building Functions [3].

THE MAIN COMPONENTS OF SMART SYSTEMS

The smart systems that can be found in a building are highly dependent on the location and size of the building, the needs of the people working there, and on the services provided for the company or for the tenants [3, 4].

The first and most crucial element is the cooling-heating ventilation (HVAC), which ensures healthy air and comfort for the people working in the building. It regulates the oxygen and carbon dioxide level, the humidity, fresh air inflow, and temperature in the building, without which, or if inappropriate values are set, the basic operation of the building and the work done inside will be impossible. For the system to work, it is essential to have sensors in the building to measure the mechanical values and the number of people in each room, where the temperature is automatically controlled if there are too many people inside, because the heat output per person raises the temperature or humidity and reduces oxygen levels.

Another important system is facility management, where the systems responsible for managing intelligent buildings are interconnected. With a digital floor plan of the building and a BIM model, all devices and systems are located precisely where they are in the building.

From the point of energy efficiency, the control of the lighting system is essential, because if inadequate lights are installed, or their operation is not automated, the consumption of the building will not be optimal. In addition, individual needs, such as operating the lamps after processing the data collected by the light sensor, can be met in this way.

The primary physical security system for a smart building is a fire alarm system that can save lives if adequately calibrated and integrated into smart solutions. Sensors can be used to measure the number of people and the level of oxygen in each room, so the system can automatically intervene with ventilation, or during an emergency, the disaster management team can receive accurate information about the place and the number of people involved in the event of a fire.

CYBER SECURITY ARCHITECTURE

The cybersecurity architecture of smart buildings is comprehensive, and it incorporates a variety of industry standards and fundamentals. Zero Trust includes Public Key Infrastructure (PKI), LAN, KNX / EIB, AirPlay, Bluetooth, WiFi, ZigBee, and Z-wave. Identifying of people and devices is the primary consideration, followed by the protection of the wired or wireless technologies used, and the encryption, authorization management, and management of guest users.

Today, cloud-based solutions are essential for high-volume data processing, as storage and computing capacity are scalable, making it easy to calculate and plan the costs. Figure 2 shows the Microsoft Azure IoT Hub's device stream model, a managed, central messaging service between the IoT applications and devices connected to the system. Millions of devices and various backgrounds, solutions can be connected to it, given that it is compatible with almost any standard and device [5].

It can handle SAS token-based or X.509 certificate-based authentication for authentication and authentication. The former establishes the connection on a symmetric key basis, while the latter establishes the connection with the TLS standard [5].

In terms of cloud-based architecture, Microsoft Azure IoT is one of the providers that can offer a complex solution to create the cyber security IoT architecture of a smart building. The reference architecture shown in Figure 3 includes three main groups – things, processing/analysis (insights), and execution/action – these groups contain tools and services that can form the complex system of a smart building. For example, aggregate and control on a cloud basis, process data, transmit, manage users, and control security.

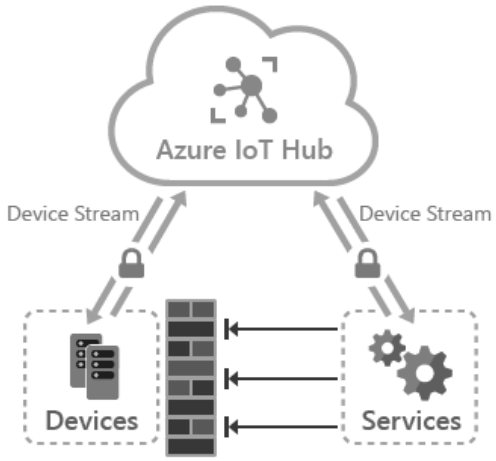

Figure 2. Microsoft Azure IoT Hub [6].

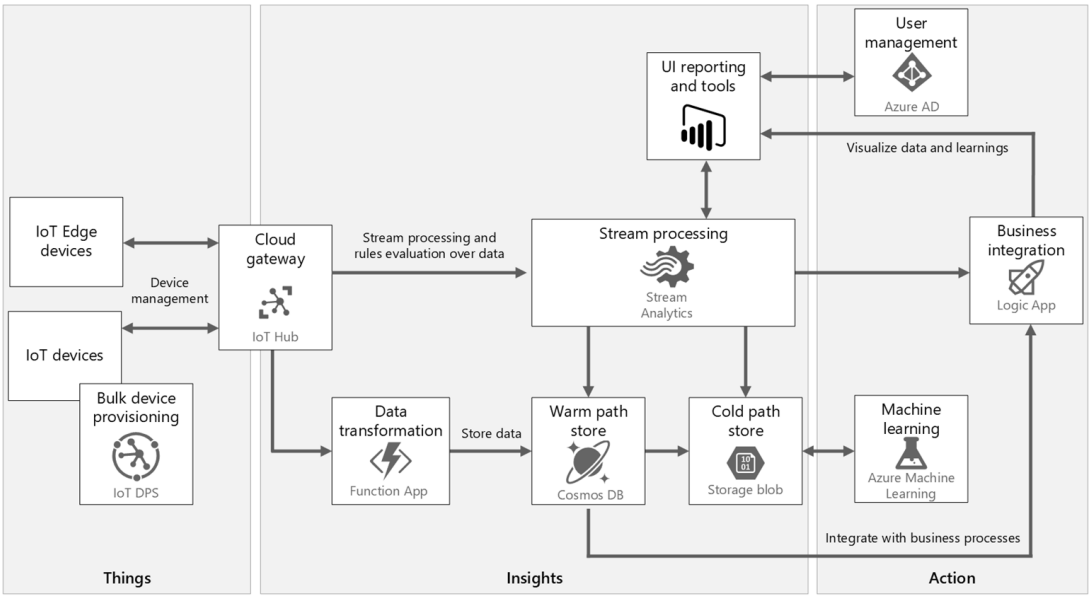

Figure 3. Microsoft Azure IoT architecture [7].

The comparison of the most common protocols in building automation should also be considered to form an idea of security (Table 1), where the most critical IT and security features are displayed. One of the main differences is network topology according to which the network can be designed, as well as the encryption protocol and algorithm within. For example, AES -128 encryption is vulnerable to brute force and man-in-the-middle (MITM) attacks, so it must be designed at a secondary security level in addition to the devices deployed.

In addition to the protocols mentioned above, Bluetooth, LonTalk, Modbus, 1-Wire, C-Bus, DALI, Insteon, oBIX, VSCP, xAP, X10, and Z-Wave are also present in the market. Several reputable manufacturers widely use them to communicate with their systems and IoT devices. These protocols include both secure and less secure ones.

CYBER SECURITY THREATS TO IOT DEVICES

Cyber security threats have been a growing threat to companies and individuals alike in recent years. Moreover, the rapid proliferation of IoT devices has added to this problem. Vedere Labs is constantly analyzing daily vulnerabilities and using a vulnerability metric to determine the top 5 IoT devices that are most at risk today (Figure 4), with projectors currently in the first

Table 1. Comparison of the various aspects of the BAS communication protocols [3].

	KNX/EIB	BACnet	ZigBee	EnOcean
ISO standard	14543-3	16484-5	-	14543-3-10
Network topology	Tree	Tree	Star, tree, mesh	Star, p2p, mesh
OSI layer	5	4	4	3
Wireless	X	X	X	X
Wired	X	X	-	X
Encryption	AES-128	AES-128 (CBC)	AES-128 (CCM*)	AES-128
Authentication	AES-CBC-MAC	HMAC	MAC	AES-CMAC
Security features easily deployed	-	-	X	X

place and printers in the last place. A number of these devices can be found in every office and in many households as well. Thus, it is relatively easy to conclude that improperly maintained devices can be potential sources of danger and primary points of intrusion in the event of a targeted cyber-attack. Currently, the highest Common Vulnerability Scoring System vulnerability is CVE-2011-4161, which affects HP printers [8].

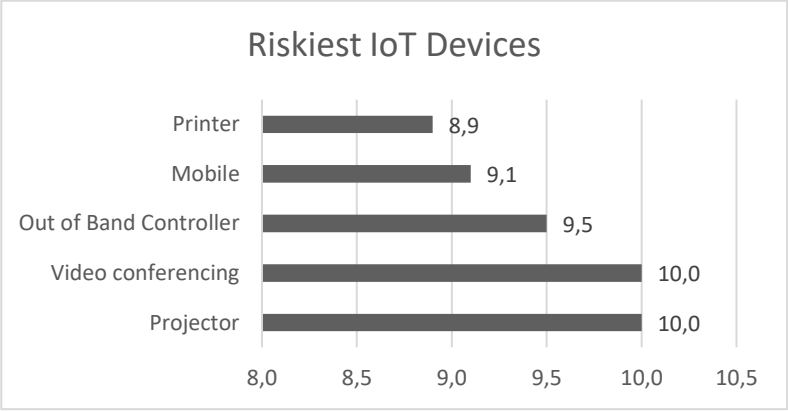

Figure 4. Riskiest IoT Devices [9].

Cyber-attacks on IoT devices have been ongoing for the past six years. Starting with the Mirai botnet attack in 2016, millions of IoT devices were infected and networked around the botnet, making it impossible to access Dyn Inc. in the U.S. and the Internet for several global companies [10]. This attack was followed by the 2017 WannaCry attack, which was a blackmail virus-based attack with a broad spectrum of attack vectors. Approximately 230 000 computers and IoT devices were infected in 150 countries. Moreover, the blackmailers demanded that cryptocurrency be issued for a ransom, which in most cases was not issued [11]. IoMT (Internet of Medical Things) devices in hospitals have also been attacked and, in many cases, made it impossible to work with the device, putting patients at risk [12]. The exposure to inadequately protected IoT devices and systems to extortion viruses is high, as the malicious code can enter the network unnoticed. In other cases, the device can even be connected to a botnet without the operator's knowledge.

The latest research from Vedere Labs is called the "R4IoT" project, where a next-generation extortion virus attack was demonstrated in a simulated environment. The bottom line is that in a vulnerable OT (operational technology) environment, the vulnerability can be exploited and accessed through a building's IT system. This attack concept is not based on file encryption by a classic blackmail virus, but on victim blackmail, where attackers threaten to leak sensitive data. Thus, a psychological method is added to the attack methods, so we can now talk about double blackmail. In another phase of the attack, the vulnerability of an IP camera can be

exploited to gain access to the IT network and see a live image of the room through the camera. This attack makes it easy to test, for example, the vulnerability of each building control system and the success of the attack, as they get a live picture of whether or not they have managed to turn off the lights or shut down the fan. In many cases, there is no such feedback for an attack. The attack consists of several stages, one of which involves placing a blackmail virus on the network, which, if activated later, will be able to extort money from the victim [13]. Separated and properly and continuously monitored systems and devices are in place to prevent such attacks, where identification, encryption, and authorization management are adequately controlled. Of course, there are so-called 0-day vulnerabilities, which can be discovered later, when there is no patch to fix them, but these systems should be protected against them. The consequences of a cyber-attack should be considered in the security system's design and the preliminary risk assessment, including the further economic, prestige, data protection, and physical consequences.

In 2022, the main threats to IoT devices were [14]:

1. Unencrypted data storage;
2. Unencrypted financial information;
3. Physical access through the IoT device;
4. Weak password and authentication;
5. Botnet and infected IoT devices.

FUTURE RESEARCH

In the future, the number of of these buildings will increase globally, which will be a significant step forward in environmental protection and energy efficiency. However, it will require a continuous supply of cyber security professionals, which is not easy now because there is a massive global shortage of IT and cybersecurity professionals. Furthermore, these professionals need specialized expertise in the protection of IoT, wireless devices, and systems, which are not always uniform or have different manufacturers, so they need to be integrated. To continue our research, we intend to examine the cyber security of smart homes as the next element of smart cities.

CONCLUSION

To summarize our research, it can be stated that the protection of smart buildings is a complex and multifaceted task, given that a building automated at this level is equipped with various IT systems, standards, and devices. Moreover, protecting these systems requires a high level of cybersecurity expertise, experience, and complex teamwork, as a cyber-attack can cause severe damage to the building and the people who work in it, if, for example, a malicious hacker attacks the elevator we are traveling in. Thus, the continuous training and development of these professionals is essential to design, maintain and continuously improve the cyber security protection of these buildings with appropriate expertise.

ACKNOWLEDGMENT

The research on which the publication is based has been carried out within the framework of the project entitled "How do we imagine? About cobots, artificial intelligence, autonomous vehicles for kids". Project no. MEC_N-141290 has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund, financed under the MEC_N funding scheme (affiliation: NextTechnologies Ltd. Complex Systems Research Institute).

REFERENCES

[1] Lechner Tudásközpont: *Okos Város Példatár*.
http://okosvaros.lechnerkozpont.hu, accessed 27th June, 2022,

[2] –: *The first one turns off the light*.
https://100.theben.co.uk, accessed 27th June, 2022,

[3] Wendzel, S., et al.: *Security and Privacy in Cyber-Physical Systems*.
Wiley & IEEE Press, 2017,

[4] Tokody, D.; Papp, J.; Iantovics, B.L. and Flammini, F.: *Complex, Resilient and Smart Systems.*
In: Flammini, F., ed.: *Resilience of Cyber-Physical Systems*. Advanced Sciences and Technologies for Security Applications. Springer, Cham, pp.3-24, 2019,
http://dx.doi.org/10.1007/978-3-319-95597-1_1,

[5] Community: *IoT concepts and Azure IoT Hub.*
https://docs.microsoft.com/en-us/azure/iot-hub/iot-concepts-and-iot-hub, accessed 27th June, 2022,

[6] Community: *MS Azure IoT Hub Device Streams*.
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-device-streams-overview, accessed 27th June, 2022,

[7] Azure Info Hub: *Azure IoT reference architecture*.
https://azureinfohub.azurewebsites.net/Architecture/Details/163371, accessed 27th June, 2022,

[8] HP: *NVD - CVE-2011-4161.*
https://nvd.nist.gov/vuln/detail/CVE-2011-4161, accessed 27th June, 2022,

[9] Vedere Labs: *Global Cyber Intelligence Dashboard*.
https://dashboard.vederelabs.com, accessed 27th June, 2022,

[10] Sándor, B.: *Vulnerability Analysis of a Smart Heating System*.
Papers on Technical Science **9**(1), 211-214, 2018,
http://dx.doi.org/10.33894/mtk-2018.09.48,

[11] Sándor, B. and Fehér, D.J.: *Examining the Relationship between the Bitcoin and Cybercrime*.
In: *2019 IEEE 13th International Symposium on Applied Computational Intelligence and Informatics*. IEEE, pp.121-126, 2019,
http://dx.doi.org/ 10.1109/SACI46893.2019.9111568,

[12] Malwarebytes: *WannaCry Ransomware.*
https://www.malwarebytes.com/wannacry, accessed 27th June, 2022,

[13] Vedere Labs: *R4IoT: Next-Generation Ransomware.*
https://www.forescout.com/resources/r4iot-next-generation-ransomware-report, accessed 27th June, 2022,

[14] IoT Business News: *Top IoT Security Threats in 2022*.
https://iotbusinessnews.com/2022/05/02/16441-top-iot-security-threats-in-2022, accessed 27th June, 2022.