

Research on data transmission technologies and information security in IoT networks

Olga Zhydka^{1†}, Myroslav Riabiyi^{2†}, Andriy Fesenko^{2†}, Lazat Kydyralina^{3†} and Tetiana Okhrimenko^{2†}

¹ State University of Information and Communication Technologies, Solomyanska Str. 7, 03110, Kyiv, Ukraine

² National Aviation University, Liubomyra Huzara ave. 1, 03058, Kyiv, Ukraine

³ NAO "Shakarim University in Semey", Shugaeva 163, 070000 Semey, Kazakhstan

Abstract

Important functions of the Internet of Things (IoT) concept include facilitating everyday life, increasing work efficiency and quality, energy saving, and more. Increasingly, data from "things" are transmitted to public communication networks and cloud services. Any objects in the physical world that can be assigned IP addresses and are capable of transmitting data can act as "things" in such a network. Various technologies and protocols are used for data transmission, with more than twenty currently available. In the near future, a large number of devices will be connected to the Internet of Things. Most of these devices will be battery-operated. One of the main characteristics is the duration of equipment operation without human intervention. To address this issue, new networks were created specifically for the Internet of Things. These networks are called LPWAN. One of the key problems is selecting the optimal method of data transmission between nodes in the Internet of Things concept. After analyzing open sources, it can be concluded that the technologies NB-IoT, Weightless, LoRa, and SigFox are promising for this goal. The subject of the research in this article is the technologies and protocols for long-distance data transmission used for transmitting information from a sensor to a cloud service in the context of the Internet of Things (IoT). The aim of the research is to review and compare the main technologies and protocols for long-distance data transmission in IoT networks. A comparative analysis of the main characteristics of long-distance data transmission protocols and LPWAN network technologies: NB-IoT, Weightless, LoRa, and SigFox, was conducted. The results of the analysis are presented in the form of a table. Experimental results have shown that the efficiency of the considered protocols and technologies depends on various communication network conditions. Currently, the choice of protocols for devices, depending on operating conditions, helps address the issue of resource savings, such as energy consumption, and ensures reliable data delivery. This is particularly important due to the spread of Internet of Things technology and the increasing number of connected devices.

Keywords


IoT, Internet of Things, network, protocol, data transmission, technologies, information security, cyber attack, cybersecurity, DDoS attack

SCIA-2024: 3rd International Workshop on Social Communication and Information Activity in Digital Humanities, October 31, 2024, Lviv, Ukraine

* Corresponding author.

† These authors contributed equally.

✉ m.o.ryabyy@gmail.com (A. Ometov); olha.zhydka@meta.ua (O. Zhydka); a.fesenko@npp.nau.edu.ua (A. Fesenko); lazat_75@mail.ua (L. Kydyralina), t.okhrimenko@npp.nau.edu.ua (T. Okhrimenko)

 0009-0009-4272-9071 (O. Zhydka); 0000-0002-9651-9135 (M. Riabiyi); 0000-0001-5154-5324 (A. Fesenko); 0000-0002-2836-0919 (L. Kydyralina) 0000-0001-9036-6556 (T. Okhrimenko)



© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

1. Introduction

Internet of Things (IoT) is a concept of a computational network of physical objects equipped with embedded technologies to interact with each other or the external environment, considering the organization of such networks as a phenomenon capable of restructuring economic and social processes, which excludes the necessity of human intervention in some actions and operations [1]. The implementation of IoT requires significant efforts and modern solutions to ensure security and privacy.

Many researchers worldwide are currently addressing security issues in the Internet of Things, especially due to a range of problems that arise during the operation of IoT devices. The article also examines issues related to ensuring access to secure networks for IoT devices. The existence of a large number of inadequately protected devices facilitates the conduct of DDoS attacks, during which household devices can be used to attack corporate systems. Some potential security threats to IoT systems are also considered. Based on the analysis of the most common attack technologies, a list of recommendations was developed to ensure the integrity of networks with IoT devices [2].

IoT is already benefiting billions of people worldwide, offering new opportunities and significant cost reductions. In the IoT concept, the key is to choose the optimal method of information transmission between nodes. By analyzing open sources, one can conclude the prospects of using technologies such as NB-IoT, Weightless, LoRa, and SigFox for these purposes.

Since IoT systems utilize devices that constantly collect and process data about the surrounding environment, they become potentially hazardous to end-users. Considering the increasing level of cybercrime, particular attention should be paid to these devices, as the threat extends beyond just data loss and may also involve the exploitation of computing resources for various cyber attacks [3].

Among the drawbacks of such systems are the necessity of using modern sensors, controllers, as well as methods and means of information transmission. Therefore, the implementation of IoT devices and the resolution of the most common problems associated with them are relevant research directions.

2. Research Analysis

The number of IoT devices continues to grow rapidly, surpassing the number of non-IoT devices globally. It is projected that by 2025, the total number of installed smart devices will reach 30.9 billion, and by 2030, 75% of all devices will belong to the IoT category [4]. However, with the increase in the number of connected devices, security issues also escalate. The interconnectivity between IoT devices has become a significant contemporary issue. Several available protocols with different performance, data transfer speed, coverage, power, and memory capacity exist for convenient connection of IoT devices to the Internet, each with its advantages and drawbacks.

Most IoT devices are expected to operate on batteries. Therefore, one of the primary requirements for such devices is the duration of autonomous operation without human intervention. To ensure the longevity of IoT device operation, new networks called LPWANs (Long Power Wide Area Networks) have been developed. These networks are characterized by

low data transmission power, allowing them to operate on batteries for extended periods. NB-IoT, Weightless, LoRa, SigFox, and other technologies are among the main technologies of these networks. The mentioned technologies provide long-term autonomous operation of devices and low cost. They are used in areas such as smart cities, agriculture, and healthcare [5]. Next, the main LPWAN technologies will be provided, and the primary security issues and possible IoT solutions to address them will be discussed.

3. Research Objective

In IoT applications, communication technologies encompass a variety of protocols, including Wi-Fi, RFID, NFC, ZigBee, Bluetooth, LoRa, NB-IoT, GSM, GPRS, 3G/4G/5G networks, Ethernet, RS232, RS485, USB, and others. Corresponding communication protocols (protocol stacks, technical standards) also include Wi-Fi (IEEE 802.11b), RFID, NFC, ZigBee, Bluetooth, LoRa, NB-IoT, CDMA/TDMA, TCP/IP, WCDMA, TD-SCDMA, TD-LTE, FDD-LTE, TCP/IP, HTTP, and others.

The research objective is to provide an overview and comparative analysis of the main technologies and protocols for long-distance data transmission in IoT networks. Additionally, the research aims to analyze the current landscape of threats relevant to IoT devices in 2023 and explore potential solutions to mitigate these threats. The utilization of diverse devices complicates cybersecurity efforts due to the complexity of the IoT architecture. Therefore, it is necessary to conduct an analysis and develop effective security measures to enable users to fully trust this technology.

4. Research Findings

The LoRaWAN technology has generated significant interest in the wireless communication field, leading to the necessity of establishing a unified standard for global low-power wide area networks (LPWANs). The abbreviation LoRa stands for "Long Range", indicating its capability to transmit data over long distances with low power consumption. LoRa was developed and patented by Semtech and is utilized in LPWANs. The LoRaWAN protocol is open, meaning it can be adopted by any company. This facilitates the proliferation of LoRaWAN technology and its utilization in various domains (Figure 1). The LoRaWAN technology holds great potential for IoT development as it enables the connection of a large number of low-power devices, opening up new possibilities for automation and control.

The LoRa modulation method is based on spread spectrum technology. This means that data is transmitted in the form of wideband pulses with a frequency that changes over time. This approach offers several advantages. Firstly, it makes the transmitter and receiver more resilient to interference. Secondly, it allows the use of inexpensive components, such as quartz resonators. LoRa operates in the sub-gigahertz frequency range, which also contributes to its energy efficiency.

With a high sensitivity level of -148 dBm, LoRa technology is indeed ideal for devices requiring low power consumption and having high communication stability requirements over long distances.

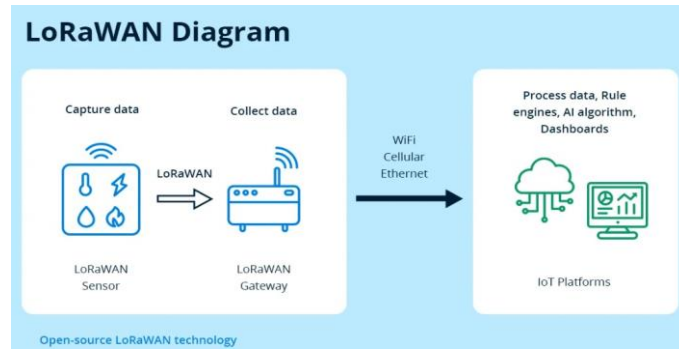


Figure 1: LoRaWAN Scheme.

NB-IoT is a cellular communication standard designed for low-power devices (Figure 2). It enables communication operators to provide Internet of Things services. NB-IoT, developed by 3GPP, can be viewed as the evolution of cellular communication towards IoT. It offers several advantages over other IoT technologies, including low energy consumption, wide coverage, and the ability for quick network modernization (NB-IoT can easily be added to existing cellular networks).

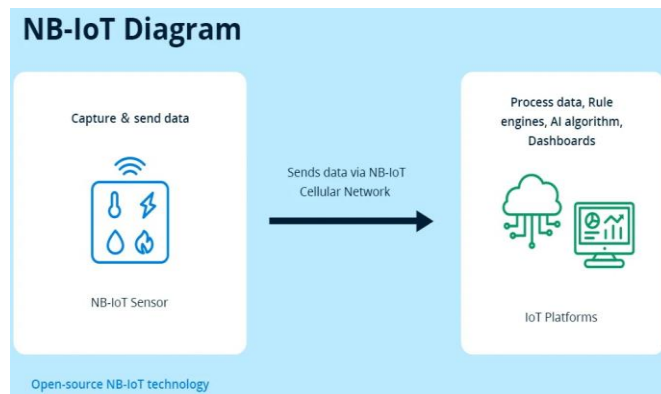


Figure 2: NB-IoT Scheme.

NB-IoT is built upon cellular networks, making it part of existing mobile operator infrastructures. This ensures wide coverage and reliable communication.

Operating in licensed spectrum, NB-IoT is more reliable and less susceptible to interference compared to unlicensed technologies like LoRaWAN.

Standardization of NB-IoT was achieved in 3GPP Release 13, ensuring compatibility and interoperability between different devices and networks.

The trend towards using embedded SIM cards, or eSIM, simplifies the installation and management of IoT device connections, providing global coverage without the need for physical SIM card replacement.

Overall, NB-IoT has the potential to become one of the key standards for connecting IoT devices to the Internet due to its advantages in low energy consumption, wide coverage, and support for existing cellular infrastructure.

Weightless-P is a low-power wireless communication technology used for the Internet of Things. It is designed for devices requiring long battery life, bidirectional communication, and support for a large number of devices. Notable features of this technology include wide coverage, network scalability, long battery life, and security.

Weightless-P supports multiple modulation types but operates within a limited range, allowing it to maintain high-quality communication even in challenging conditions. One Weightless-P base station can serve more devices than a base station of another LPWAN technology. Additionally, Weightless-P base stations have full control over the network and devices, enhancing security and reliability.

Compared to LoRa and SigFox, Weightless-P is a more advanced technology. It supports guaranteed message delivery, ensuring messages reach the end device even under weak signal conditions and in the presence of obstacles. This helps avoid message retransmissions, saving device battery power. Weightless-P also utilizes adaptive data rate support, meaning the data transmission speed adapts based on the device's distance from the base station. The more optimized and compact Weightless-P protocol reduces system costs and operational complexity by requiring less hardware and software.

These features increase network performance and extend the battery life of devices. Additionally, Weightless-P is noted for its optimized and compact protocol compared to NB-IoT and other cellular M2M systems, further reducing system costs and operational complexity.

The technology is used in various surveillance systems, health monitoring, smart devices, and other fields, providing reliable long-distance communication with low energy consumption, making it attractive for various IoT applications.

Sigfox is another significant player in the LPWAN market, competing with LoRaWAN and NB-IoT for IoT connectivity leadership. It utilizes ultra-narrowband technology in unlicensed spectrum, offering a simple, energy-efficient, and cost-effective solution suitable for applications requiring occasional transmission of small data packets. While its deployment may lag behind LoRa and NB-IoT, Sigfox is already present in over 70 countries, particularly popular in logistics and supply chain tracking, where reliable global coverage is essential. Sigfox stands out for its simple setup, exceptional energy efficiency allowing for autonomous operation for many years, and wide availability. It can transmit small data packets almost anywhere, a capability that many competitors in the high-speed LPWAN segment lack.

Sigfox is a wireless communication technology enabling connectivity for a large number of low-power devices. Its network architecture resembles that of cellular communication operators (GSM and GPRS) but with some differences. Firstly, Sigfox operates in sub-gigahertz frequency bands, enhancing its energy efficiency. Secondly, it uses a simpler modulation method, further contributing to its energy efficiency.

Sigfox has a large coverage radius, reaching up to 30-50 km in rural areas and 3-10 km in urban areas. It has the potential for widespread application across various fields, allowing connectivity for numerous low-power devices, thus opening up new possibilities for automation and control.

Sigfox uses narrowband frequency for data transmission between devices and base stations. This allows it to be highly energy-efficient, which is crucial for low-power devices.

Sigfox devices transmit their messages to Sigfox base stations. These base stations then relay the data to Sigfox cloud servers. Sigfox cloud servers transmit the data to client servers and IT platforms via application programming interfaces (APIs).

Sigfox's technology aims to provide low-cost device connectivity and wide coverage. This feature makes it an ideal choice for applications requiring extensive coverage and significant cost constraints.

With the increasing number of connected devices, the need for their protection grows. The first large-scale attacks on IoT devices using malware were recorded back in 2008, and since then, such attacks have only increased.

To prevent attacks on IoT devices, it is essential to identify various types of attacks that cybercriminals may use.

1. One such type of attack is a *DDoS attack*. DDoS (Distributed Denial of Service) attacks pose a significant threat to IoT devices. In these attacks, a botnet composed of compromised devices sends a large number of requests to the target system or network, attempting to overwhelm their resources. Due to the high volume of requests coming from the botnet, the network or target system may become overloaded, resulting in decreased performance or even complete failure. A well-executed DDoS attack can lead to system errors or security vulnerabilities that could be exploited to gain unauthorized access to the system. Cybercriminals can compromise IoT devices and use them to create a botnet that executes DDoS attacks. This is particularly dangerous because IoT devices may be less secure and less noticeable to users. Attackers may use compromised IoT devices for internal attacks within the local network. This can lead to the compromise of the entire network's security and the loss of confidential information. In the first half of 2023 alone, analysts identified over 700 announcements of DDoS attack services on various darknet forums (Figure 3).

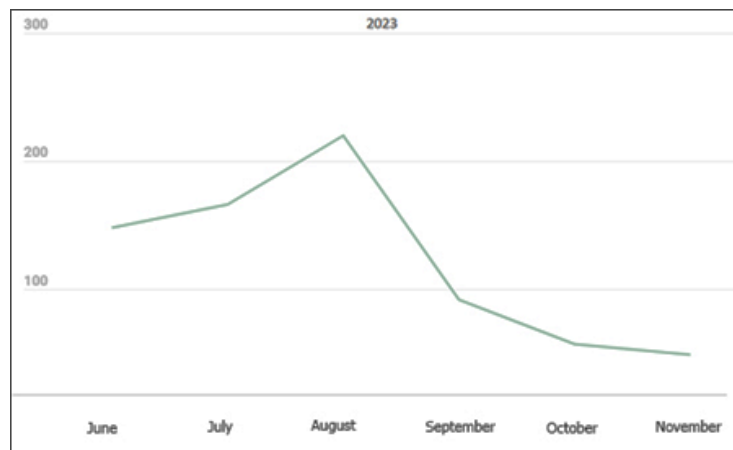


Figure 3: Distribution of the number of publications related to DDoS attack services by month, 2023.

2. *Exploits in software* pose a serious threat to IoT devices and can lead to dangerous consequences. Cybercriminals may exploit known vulnerabilities in device software to carry out attacks. This can include open ports, authentication flaws, inadequate access controls, and more. Not all IoT device manufacturers timely provide software updates. This renders devices vulnerable to attacks, as attackers may exploit vulnerabilities that have been fixed in newer versions of the software. Not all manufacturers provide sufficient information to users about the software used in their devices. This can complicate the process of detecting and fixing vulnerabilities, as users may be unaware of potential security threats [9].

3. *Man-in-the-Middle (MitM)* attacks are among the most sophisticated and widely used cyberattack methods. It involves an attacker inserting themselves between communicating parties, typically the sender and the receiver device, and intercepting and manipulating the communication flow. Attackers can alter data during its transmission between devices. This allows them to influence the behavior of devices and manipulate communication outcomes. Many smart devices are often unencrypted, making them particularly vulnerable to MitM attacks. With the obtained data, attackers can gain unauthorized access to systems, devices, or networks, leading to leakage of sensitive information or execution of unwanted actions [10].

4. *Physical tampering*: simply connecting a USB flash drive with malicious code to an external IoT device can be enough for a cybercriminal to spread malicious software across the network and eavesdrop on communications passing through it.

5. *Brute-force attacks*: the fact that companies usually do not pay enough attention to the password security of IoT devices makes them vulnerable to potential brute-force attacks. Often, IoT device passwords remain unchanged after installation, making it easy for attackers to guess them. During the first half of 2023, 97.91% of password brute-force attempts detected by honeypots were related to the Telnet protocol and 2.09% to SSH. The majority of infected devices conducting these attacks were located in China, India, and the USA (Figure 4), with China and Pakistan leading in the number of attacks [11].



Figure 4: Top 10 Countries and Territories with the Majority of Devices Attacking Honeypots, 2023.

6. *Firmware theft* poses a significant threat to the security of IoT devices. The firmware, which controls the operation of the device, may contain critical data, settings, and serve as a key security element. Attackers can use stolen firmware to gain control over the device, including executing malicious commands or installing additional malware. If the stolen firmware contains confidential data, such as credentials or encryption keys, attackers can access this information and exploit it for their purposes, including leaking confidential information. Attackers may modify the stolen firmware to include malicious software. Subsequently, they can distribute this software to other devices running on the same or similar firmware.

5. Discussion of Research Findings

Based on the analysis of open sources, conclusions can be drawn regarding the suitability of the following technologies for the stated purposes: NB-IoT, Weightless, LoRa, SigFox (see Table 1).

Table 1

The comparative characteristics of data transmission technologies for long distances in IoT networks

Characteristics	LoRaWAN	SigFox	NB-IoT	Weightless-P
Modulation Method	CSS	DBPSK/GFSK	GFSK/BPSK/QPSK	GMSK/ PSK
Range	ISM	ISM	Licensed	ISM
Speed	0.3-50 kbps	100 kbps	UL: 1-144 kbps DL: 1-200 kbps	0.2-100 kbps (adaptive)
Bandwidth	Narrow-band. Up to 500 kHz	Narrow-band. 100 kHz	Narrow-band. 200 kHz	Narrow-band. 12.5 kHz
Maximum autonomous operation time of devices	>10 years	Up to 20 years	Up to 10 years	3-5 years
Frequency	868,8 MHz (Europe) 915 MHz (USA) 433 MHz (Asia)	868,8 MHz (Europe) 915 MHz (USA)	800/900/ 1800 MHz	169/433/470/780/868/915 MHz
Security	AES-64/128	AES with HMACs	AES-256	AES-128/256
Range	Up to 2.5 km in urban areas Up to 45 km outside the city	Up to 10 km in urban areas Up to 50 km outside the city	Up to 2 km	Up to 2 km in urban areas

LoRaWAN and NB-IoT are indeed two key technologies for the development of the Internet of Things, especially in large-scale networks where extensive coverage and low power consumption are needed. Below is a comparison diagram of some characteristics of these technologies (Figure 5) [6].

By 2024, LoRaWAN will have a global footprint with over 170 operators in 181 countries. According to GSMA data, NB-IoT has gained greater regional popularity with deployments by 124 operators in 64 countries, mainly in Asia and Europe. LoRaWAN led chipset shipments in 2022 at 65.9 million, including NB-IoT at 22.4 million, with projected growth of all shipments by 20% by 2027 (Figure 3) [9]. LoRaWAN is the leading LPWAN technology for IoT [13].

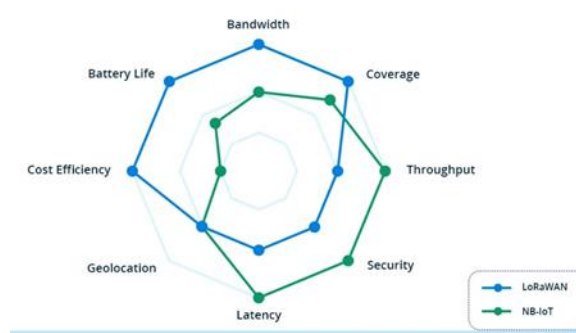


Figure 5: Comparison diagram of LoRaWAN and NB-IoT technologies as of the year 2024.

From the above-mentioned vectors of attack on IoT, it can be concluded that the main components of IoT systems are quite vulnerable to attacks by malicious actors. Regardless of the scale and type of environment in which an IoT system is embedded, security should be considered at the design stage to improve its integration. A particular challenge for engineers and information security officers is that due to the technological characteristics of IoT, it is not possible to install an agent to check for infections or vulnerabilities.

After analyzing open sources, several key recommendations can be made to prevent attacks on devices and generally reduce company security risks.

1. Attack surface management, inventory, and monitoring of all devices. During IoT security planning, one of the main tasks should be to create a map of connected devices for inventory purposes. Security teams should know the exact number of devices in use, as well as manufacturer identifiers, serial numbers, hardware versions, and firmware. Real-time monitoring, analysis, and reporting are extremely important for organizations to be able to manage IoT risks. However, traditional endpoint security solutions typically use technology called software agents, which are not suitable for IoT devices. Fortunately, there are better modern approaches - agentless solutions (such as DeviceTotal) for attack surface monitoring. They provide real-time risk assessment, continuously analyzing the behavior and status of all connected IoT devices. Some solutions of this kind even allow managing the surface of pre-cognitive attacks, taking into account the risks of potential "zero-day" attacks. These security tools enable organizations to leverage the full benefits of IoT technology, addressing its main drawback - insufficient security [14].
2. Network segmentation. In the event of a successful cyber attack, an attacker can gain access to the entire organization's network. Segmentation prevents this by limiting the attack surface and minimizing damage. Network segmentation is the process of dividing the internal network into several separate subnets. Although segments may occasionally communicate with each other, they are usually independent and isolated from each other. This method allows focusing more attention on individual parts of the network that contain the most critical data for their enhanced protection.
3. Setting up reliable passwords for IoT. Many IoT devices come with weak pre-installed passwords that are very easy to guess. As soon as an IoT device is first registered on the network, the best practice is to change its pre-installed password to something much more complex. The new password should be resistant to guessing, unique for each

secured device, and comply with the password management policies of your IT security team.

4. Physical protection of all IoT devices. Physical protection of devices is very important because devices accessible from the outside can be subject to physical tampering by attackers seeking unauthorized access or loading malicious software into the system. Therefore, it is necessary to ensure a secure location for the device to prevent unauthorized access to it.
5. Timely firmware updates. New firmware versions may contain fixes for existing software vulnerabilities in the device. Therefore, their regular update will significantly improve the overall security of IoT. However, updates should also be checked for counterfeiting, as attackers may download malicious software onto the device under the guise of an update. Another aspect of updates is vulnerabilities in official updates. It is necessary to monitor the versioning and keep the latest secure firmware version, automated firmware analysis systems will help with this.

6. Conclusions

Choosing the optimal LPWAN technology depends on specific application needs. For example, NB-IoT is a good choice for applications requiring long autonomous operation and low cost, such as smart cities and agriculture. Weightless is a good choice for applications requiring low cost and high throughput, such as industry and logistics. LoRa and SigFox are good choices for applications requiring very low cost and very long autonomous operation, such as healthcare and environmental monitoring.

The history of data transmission has divided it into several types: wired, cable, and wireless. Despite the development of wireless systems, they need to be combined with other types of data transmission, as well as with each other, to increase efficiency.

The Internet of Things brings many benefits but also creates a number of security challenges. These challenges include device vulnerabilities, data privacy issues, and network insecurity.

To address these issues, companies that develop applications for the Internet of Things can be consulted. They can implement reliable security measures such as device authentication, encryption, and regular software updates.

Furthermore, IoT devices should be designed with security in mind from the outset, and companies should have a clear and transparent data privacy policy. IoT application developers can ensure the security of devices and the data they collect and transmit.

Following the recommendations above will help to safely utilize IoT devices, harnessing their benefits to the fullest while minimizing risks. However, it's important to remember that cyberattacks are constantly evolving, so it's crucial to stay informed about new developments in cyberspace and regularly update security measures using cutting-edge solutions for device monitoring and attack surface analysis.

References

- [1] Aleksander M., Korchenko O., Karpinski M., Odarchenko R., Vulnerability investigation for Internet of things sensor subnetworks architecture for different types of attacks, Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 1, p. 12-19. URL: <https://er.nau.edu.ua/bitstream/NAU/36403/1/10448-26997-1-SM.pdf>

- [2] D. Didenko, Common attacks on IoT and protection against them, 2023. URL: <https://corewin.ua/blog/attacks-on-iot-how-protect/>
- [3] Agentless vulnerability management for IoT and OT. URL: <https://corewin.ua/blog/agentless-vulnerability-management-for-iot-and-ot/>
- [4] A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications. URL: <https://arxiv.org/pdf/1802.02041.pdf>
- [5] Overview of IoT protocols and how to choose the best IoT protocol. URL: <https://www.dusuniot.com/uk/blog/best-wireless-protocol-for-your-iot-project/>
- [6] LoRaWAN VS NB-IoT: How Do They Compare and Differ: URL: <https://www.mokosmart.com/uk/lorawan-vs-nb-iot-how-do-they-compare-and-differ/>
- [7] Sigfox Technology URL: <https://www.betasolutions.co.nz/Blog/17/Sigfox-Technology-Review>
- [8] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, A. Selcuk Uluagac, A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications, 2018. URL: <https://arxiv.org/pdf/1802.02041.pdf>
- [9] P. Saxena, The advantages and disadvantages of Internet Of Things, 2016. URL: <https://e27.co/advantages-disadvantages-internet-things-20160615/>
- [10] IoT security guide. URL: <https://www.dsci.in/files/content/knowledge-centre/2023/IoT-Security-Guide.pdf>
- [11] Gloukhovtsev, IoT_Security_Challenges_Solutions_and_Future_Prospects, 2018KS URL: https://education.dell.com/content/dam/dell-emc/documents/en-us/2018KS_Gloukhovtsev-IoT_Security_Challenges_Solutions_and_Future_Prospects.pdf
- [12] V. Kumar, IoT Security Challenges and Best Practices. URL: <https://www.happiestminds.com/wp-content/uploads/2020/12/IoT-Security-Challenges-and-Best-Practices.pdf>
- [13] Briefing for IoT Solution Specialists: Using LoRaWAN® in Smart Buildings, Cities & Utilities. URL: <https://lpwaninfo.com/>
- [14] Biggest security challenges & solutions for IoT. URL: <https://www.peerbits.com/blog/biggest-iot-security-challenges.html>