The Internet of Things (IoT) in World Practice: Review and Analysis

Myroslava Vlasenko[1], Yurii Khlaponin[2]

Kyiv National University of Construction and Architecture,
Povitriflotskyi Ave., 31, Kyiv, Ukraine, 03037
[1] bee.130974@gmail.com, orcid.org/0000-0001-6953-1078
[2] y.khlaponin@gmail.com, orcid.org/0000-0002-9287-0817

Received 30.10.2023, accepted 04.12.2023
https://doi.org/10.32347/uwt.2023.13.1202

Abstract. This article explores the contemporary realm of the Internet of Things (IoT) and its influence on society and the economy. The primary emphasis lies in examining the principal patterns within the realm of IoT, encompassing the escalation of connected device quantities and the utilisation of 5G networks. The article encompasses various facets, including an overview of the evolution and possibilities of IoT, encompassing the advancement of intelligent urban areas and the influence of 5G networks. The analysis of threats and vulnerabilities related to this technology focuses on detecting common flaws, including weak passwords, unsecured network services, and inadequate privacy measures.

Furthermore, the essay presents concrete hazards in diverse sectors that employ IoT technology. Particular emphasis is given to potential cybersecurity vulnerabilities in healthcare, manufacturing, agriculture, retail, transport and logistics, energy, and smart cities. These businesses have distinct challenges and hazards due to incorporating IoT technologies.

The authors also analyse the substantial financial commitment to IoT and its profound influence on the worldwide economy, including data on the expansion of the IoT market and investments in IoT technologies and smart cities. The findings emphasise that the Internet of Things (IoT) substantially influences society and the economy. However, it necessitates meticulous consideration of cybersecurity and privacy concerns. The authors underscore the significance of creating efficacious cyber security policies to safeguard against the possible hazards presented by IoT technology.

Myroslava Vlasenko
Post Graduate Student, Kyiv National University of Construction and Architecture, faculty of automation and information technology, specialty: 126 “Information systems and technologies”

Yuriy Khlaponin
Head of the Department of Cyber Security and Computer Engineering, Doctor of Technical Science, Professor

Keywords: Internet of Things (IoT), Cyber Security, Threats and Vulnerabilities, Economic Impact.

INTRODUCTION

The Internet of Things (IoT) has been developing at lightning speed in recent years. IoT is a system of interconnected devices connected to the Internet that collect, process and transmit data. The Internet of Things is the most expansive realm within technological advancements, yet the substantial potential of IoT is accompanied by considerable challenges in cybersecurity. This assertion presupposes that 'technological development' encompasses various sectors. However, it's essential to note that the term 'technological development' is commonly used to describe the overall progress in various technological domains.

The escalating number of interconnected IoT devices introduces fresh concerns regarding the privacy and security of transmitted and received

data, as well as the integrity of the IoT device itself. This arises from the fact that many IoT devices possess restricted resources and functionalities, rendering them more susceptible to cyber attacks. Unlike a simple tool like a hammer, IoT devices often process sensitive information and use default settings, creating an environment where cybercriminals can exploit vulnerabilities and launch attacks to gain access to sensitive data or take control of devices.

Ensuring cybersecurity in the implementation of the Internet of Things (IoT) requires consideration of scientific models and methods that can help avoid potential cyber attacks that could harm IoT devices, users, and individual organizations.

This article aims to provide a deep understanding of the state of affairs in the field of IoT and cyber security, which is an important foundation for further research and development of security strategies in the rapidly growing digital age. The article aims to provide a systematic analysis of the current state of IoT implementation in the modern world and emphasize its crucial influence on cybersecurity. This goal closely aligns with the previously stated objectives.

TRENDS IN THE IOT WORLD

Entering the era of digital transformation, the Internet of Things (IoT) is actively changing our perception of the world and the way we interact with it. This technology turns ordinary devices into smart ones, allowing them to collect and share data in real time.

Forecasts indicate that the number of devices connected to the Internet of Things will grow rapidly in the coming years. More and more industries and business areas will adopt IoT to improve efficiency and competitiveness [5].

Smart cities are becoming centers of IoT technologies. Urban infrastructure, security systems, transport management and many other aspects are becoming "smart", thanks to which cities become more comfortable and efficient for the lives of residents.

The emergence of 5G networks gives a new impetus to the development of IoT. High speed and low latency allows you to connect more devices and implement more complex applications [9].

Governments and international organizations are actively working to develop IoT regulations and standards to ensure security and interoperability [4].

The fast development and adoption of IoT technologies over the past few years have transformed IoT security from a rather new market segment into a critical enabler of digital transformation. In 2022, the IoT security market was valued at over five billion U.S. dollars and was forecast to be four times higher by the end of 2027. The rising number of IoT devices has led to a dramatic expansion in the number and variety of cyber-attacks since a company’s entire security network can be significantly weakened by the lack of measures or wrongly implemented policies [10].

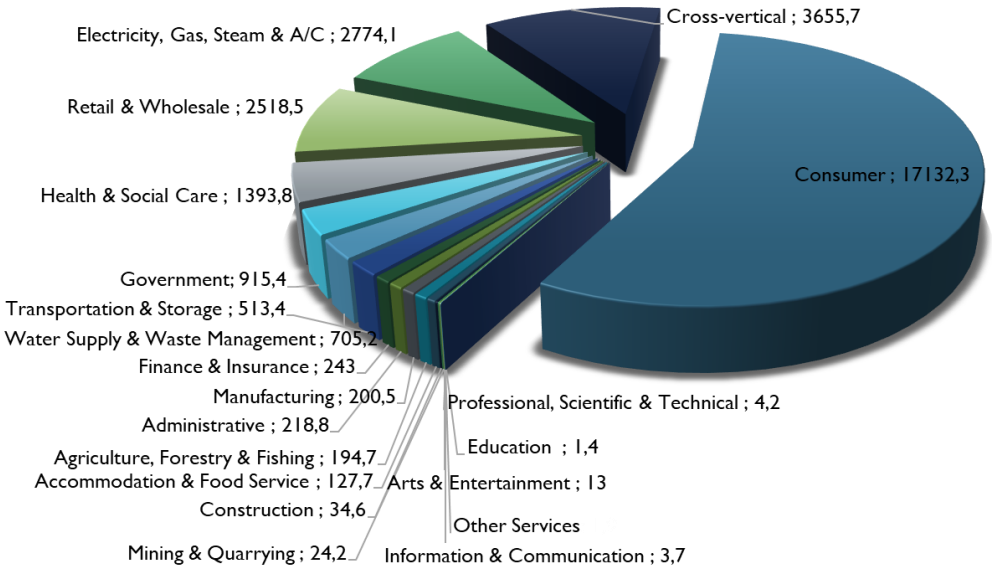

Fig. 1. Number of devices (in millions) connected to the Internet of Things (IoT) worldwide in 2030 by industry

The consumer sector is expected to dominate the number of Internet of Things (IoT) connected devices in 2030, with 17 billion connected devices worldwide (fig. 1). This number of connected devices within the consumer sector is forecast to more than triple compared to 2019. This impressive growth shows how the Internet of Things (IoT) is becoming a necessary part of everyday life and business environments, providing many opportunities for convenience, efficiency and innovation [5].

IOT THREATS AND VULNERABILITIES

The Internet of Things (IoT) has always been an area with a strong focus on innovation and convenience. However, as the number of connected devices grows, so do cybersecurity threats. When assessing the state of IoT adoption, the potential risks posed by this technology cannot be ignored.

We will now take a detailed look at the 10 most common IoT vulnerabilities in light of the growing number of cyberattacks. Table 1 shows exactly at which levels threats to these vulnerabilities exist [3].

As IoT gains widespread popularity, both manufacturers and users can reap the maximum benefits only if the devices are fortified with strict security measures. These devices require manufacturers to have advanced programming knowledge compared to traditional software. Unfortunately, security is not a top priority when building IoT devices, as most manufacturers race to reach consumers before the competition.

Table 1. The most common vulnerabilities in the Internet of things at all levels of architecture

Security issues	Application or GUI layer	Business level	Data processing level	Network level / data transport	Sensory level / level of perception
Weak, guessable, or hard-coded passwords	+				
Unsecured network services	+	+	+		
Unsecured ecosystem interfaces	+	+			
Lack of secure update mechanisms		+			
Use of unsafe or outdated			+	+	

Security issues	Application or GUI layer	Business level	Data processing level	Network level / data transport	Sensory level / level of perception
components					
Insufficient privacy protection	+	+	+	+	+
Unsafe data transmission and storage	+	+	+	+	
Lack of device management					+
Dangerous default settings	+	+		+	
Lack of physical protection	+	+	+	+	+

1. **Weak, guessable, or hard-coded passwords:** IoT devices with weak default passwords are vulnerable to cyber-attacks. Manufacturers should ensure that passwords are properly configured to avoid attacks through standard passwords.
2. **Unsecured network services**: Vulnerabilities in network services can provide a pathway for unauthorized access. Attackers can compromise the system due to weak network services.
3. **Insufficient authentication of interfaces:** Lack of proper authentication on the interfaces of IoT devices creates opportunities for unauthorized access.
4. **Lack of secure updating:** Failure to securely update devices leaves them vulnerable to known threats.
5. **Using unsafe or outdated components:** Using outdated or unsafe components can lead to vulnerabilities at various system levels.
6. **Inadequate privacy protection:** Lack of adequate information encryption can lead to leakage of sensitive data.
7. **Insecure data transmission and storage:** Inadequate data encryption can put data at risk of leakage.
8. **Lack of device management:** Failure to effectively protect all connected devices can expose the system to threats.
9. **Insecure default settings:** Having standard default settings can lead to vulnerabilities.
10. **Lack of physical protection:** Lack of physical access protection can allow attacks through direct access to devices.

This condensed text provides an overview of IoT threats and vulnerabilities, highlighting the main points.

IOT CYBERSECURITY IN VARIOUS INDUSTRIES

The Internet of Things (IoT) provides many opportunities to improve and optimize various industries, including industry, medicine, transportation, agriculture, and many others. However, as IoT applications grow, so do the number of potential cybersecurity threats.

In the following table, we look at potential cybersecurity risks in specific industries where IoT is used. This information is essential to understanding what challenges different industries may face and how they can be addressed to ensure safety and security [2].

Table 2. Potential cybersecurity risks in some industries where IoT is used

Industry	Examples of IoT usage	Potential cybersecurity risks
Health care	Patient condition monitoring and remote consultations. Tracking of medical equipment and drugs.	Leakage or unauthorized access to medical data. Attacks on medical devices and software.
Production	Automation of production processes and monitoring of equipment condition. Supply chain optimization and equipment management.	Vulnerabilities in network equipment. Threats to the integrity of data and production processes.
Agriculture	Monitoring of soil moisture and other parameters. Automation of watering and dosing of resources.	Vulnerabilities of monitoring systems and controllers. Unauthorized access to agricultural data.
Retail	Inventory tracking systems and optimization of inventory management. Personalized offers for customers based on purchase data.	Threats to the security of customer data and payment information. Possibility of attacks on points of sale and online platforms.
Transport and logistics	Monitoring of fleets and vehicles. Optimization of logistics operations and cargo tracking.	Attacks on automotive systems that can lead to road hazards. Unauthorized access to traffic data and logistics operations.
Energy and communal services	Monitoring of energy consumption and optimization of its production and distribution. Management of communal services and resources (light, water, gas).	Threats to energy systems and networks. Risk of illegal access to utility systems.
Smart houses and cities	Management of energy consumption in smart homes. Monitoring of public safety and transport systems in smart cities.	Threats to the privacy of residents and data of city systems. Risk of data misuse and illegal access to networks of smart homes and cities.

An analysis of the potential risks to cyber security in various industries where the Internet of Things (IoT) is used shows the importance of a careful and comprehensive approach to ensuring security in these sectors. The growing number of connected devices and the increase in volumes of digital information create new opportunities for attacks and threats to the privacy, integrity and availability of data.

Every industry has its own unique risks, and with that in mind, effective cybersecurity strategies must be developed and implemented. It is important to strengthen measures to monitor, detect and respond to possible threats, as well as to provide training and increase the awareness of personnel in the field of cyber security.

Ensuring cyber security in IoT industries is a critical task as these technologies become an increasingly integral part of our daily lives and society as a whole. The need to improve cybersecurity measures is constantly increasing, and only with the joint efforts of industry experts, manufacturers and regulators will we be able to ensure reliable protection of these important systems in the future.

THE ECONOMIC IMPACT OF IOT

Today, more and more organizations are investing in the Internet of Things (IoT), and as of May 2020, the number of such organizations was 2,552,000 in Europe. The volume of financing of these initiatives exceeded five

billion US dollars. In addition, in 2019, spending on the development of smart city technologies worldwide reached 104 billion US dollars [7].

The total global Internet of Things (IoT) market was estimated to be approximately US$182 billion in 2020 and is projected to grow to more than US$621 billion by 2030, tripling its revenue in ten years (fig.2). The number of IoT-connected devices worldwide is projected to triple during this time frame [8].

China is currently the region with the largest market share of the Internet of Things, with North America and Europe occupying the second and third positions in 2020. However, the market in the Greater China region is forecast to weaken slightly over the next ten years, with both North America and Europe closing the revenue gap [8].

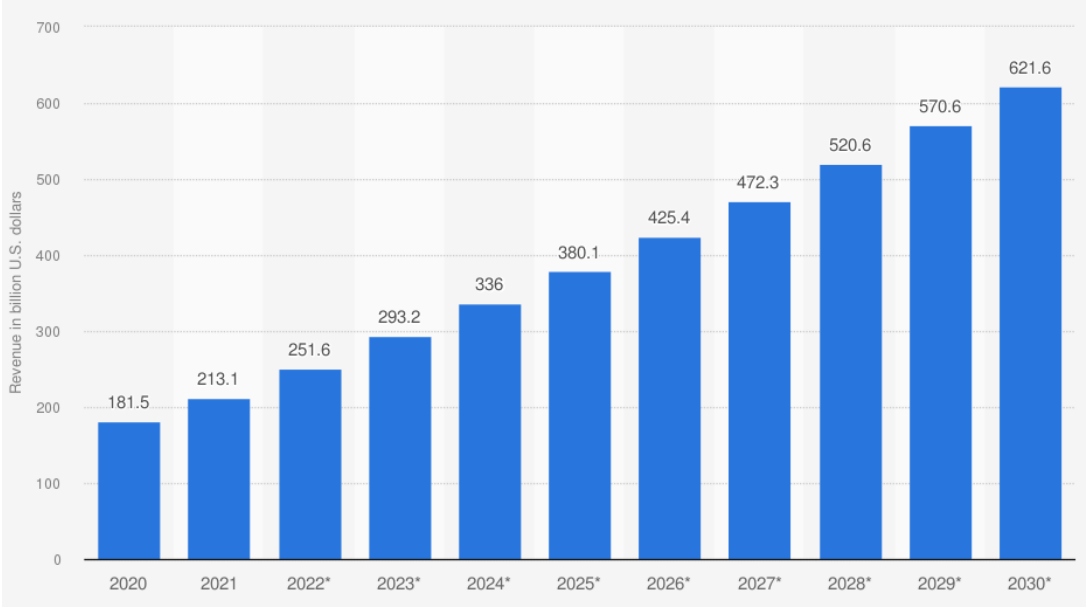

Fig. 2. Total annual revenue of the Internet of Things (IoT) worldwide from 2020 to 2030 (in billions of US dollars)

This economic growth in the field of IoT shows the significant impact of this technology on the global economy. Organizations that invest in the development and implementation of IoT solutions gain new opportunities to optimize processes, increase productivity and improve customer service.

The development of the Internet of Things also has the potential to solve many of today's global challenges, including the implementation of sustainable energy solutions, improving the quality of life in cities, increasing resource efficiency and reducing environmental impact.

All these indicators indicate that the Internet of Things is already transforming our world and will have an even greater impact in the future, creating new opportunities and challenges for business, technology and society as a whole.

CONCLUSIONS

Overall, the Internet of Things has a powerful impact on our society and economy, but requires proper attention to cybersecurity and privacy issues. The Internet of Things (IoT) is becoming a key component of our digital lives and modern businesses. It enables devices to connect and collect data in real-time, driving efficiency, convenience and innovation. Trends in the IoT world indicate a rapid growth in the number of connected devices and the expansion of their applications in various fields, including agriculture, manufacturing, transportation, and healthcare. The emergence of 5G networks and the growth of data volumes contribute to the development of IoT. IoT threats and vulnerabilities pose a serious cybersecurity challenge. Weak passwords, insecure network services, insufficient privacy protections, and other issues can lead to data leaks and incidents.

In industries using IoT, there are potential cybersecurity risks, such as medical data leaks in healthcare, threats to data integrity in manufacturing, and the possibility of point-of-sale attacks in retail. The economic impact of IoT is extremely significant, with large investments and expected market growth in the near future. Adopting IoT can lead to improved productivity and increased profits.

REFERENCES

1. **J. M.,** «Internet of Things: What It Is, How It Works, Examples and More», JUST Creative, 27 February 2023. Available: https://justcreative.com/internet-of-things-explained/.
2. **«What Is IoT (Internet of Things)? »,** ©2023 Cisco Systems, Inc. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-iot.html?dtid=osscdc000283#~iot-in-industries.
3. **«Guide To OWASP IoT Top 10 For Proactive Security»,** AppSealing. Available: https://www.appsealing.com/owasp-iot-top-10/.
4. «Internet of Things, IoT», IT-Enterprise – your one-stop ecosystem for reengineering | it.ua. Available: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot.
5. **L. S. Vailshery,** «Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by vertical», 27 July 2023. Available: https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/.
6. **L. S. Vailshery,** «Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025 (in billions) », 6 September 2022. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/.
7. **L. S. Vailshery,** «Prognosis of worldwide spending on the Internet of Things (IoT) from 2018 to 2023 (in billion U.S. dollars) », 26 July 2023. Available: https://www.statista.com/statistics/668996/worldwide-expenditures-for-the-internet-of-things/.
8. **L. S. Vailshery,** «Internet of Things (IoT) total annual revenue worldwide from 2020 to 2030 (in billion U.S. dollars) », 27 July 2023. Available: https://www.statista.com/statistics/1194709/iot-revenue-worldwide/.
9. **Taylor P.,** «Forecast of cellular IoT connections share worldwide in 2025, by vertical industry»; December 2019. Available: https://www.statista.com/statistics/443164/cellular-m2m-and-iot-market-revenue-forecast-in-the-us/.
10. **Alsop T.,** «Topic: Tech trends 2023», 21 February 2023. Available: https://www.statista.com/topics/9025/tech-trends/#topicOverview.

Інтернет речей (IoT) у світовій практиці: огляд та аналіз

Мирослава Власенко, Юрій Хлапонін

Анотація. Ця стаття досліджує сучасну сферу Інтернету речей (IoT) та його вплив на суспільство та економіку. Основний акцент робиться на вивченні основних моделей у сфері IoT, що охоплює ескалацію кількості підключених пристроїв і використання мереж 5G. Стаття охоплює різні аспекти, включаючи огляд еволюції та можливостей Інтернету речей, охоплюючи розвиток інтелектуальних міських районів і вплив мереж 5G. Аналіз загроз і вразливостей, пов'язаних із цією технологією, зосереджується на виявленні поширених недоліків, зокрема ненадійних паролів, незахищених мережевих служб і неадекватних заходів конфіденційності.

Крім того, есе представляє конкретні небезпеки в різних секторах, де використовується технологія IoT. Особлива увага приділяється потенційним вразливостям кібербезпеки в охороні здоров'я, виробництві, сільському господарстві, роздрібній торгівлі, транспорті та логістиці, енергетиці та розумних містах. Ці підприємства мають різні виклики та небезпеки через впровадження технологій IoT.

Автори також аналізують значну фінансову прихильність до IoT та його глибокий вплив на світову економіку, включаючи дані про розширення ринку IoT та інвестиції в технології IoT та розумні міста. Висновки підкреслюють, що Інтернет речей (IoT) суттєво впливає на суспільство та економіку. Однак це вимагає ретельного розгляду питань кібербезпеки та конфіденційності. Автори підкреслюють важливість створення ефективних політик кібербезпеки для захисту від можливих небезпек, створених технологією IoT.

Ключові слова: Інтернет речей (IoT), кібербезпека, загрози та вразливості, економічний вплив