THREATS TO CYBERSECURITY IN THE INTERNET OF THINGS (IoT) ERA[1]

Ivana Baltezarević

ORCID: https://orcid.org/0000-0003-4605-1420

ivana.baltezarevic@gmail.com

Associate Professor, Faculty of Law, Megatrend University, Belgrade, Republic of Serbia

Radoslav Baltezarević

ORCID: https://orcid.org/0000-0001-7162-3510

radoslav@diplomacy.bg.ac.rs

Institute of International Politics and Economics, Belgrade, Republic of Serbia

Abstract

Devices that have sensors, processors, software, and other technologies that connect to other devices and systems over the internet or other communication networks to exchange data are referred to as Internet of Things, or IoT. With the use of IoT, machines can finish laborious tasks without assistance from humans. This technology has a huge impact on our daily lives by improving its functionality, convenience, and efficiency. They are changing not only how people use their homes and personal electronics but also how the healthcare, IoT manufacturing, and transportation sectors operate. However, one of the main issues is that a lot of IoT devices don't even have basic security protections. The acceleration in the use of IoT devices has drawn the attention of cybercriminals as well. These IoT attacks represent malicious attempts to exploit weaknesses in internet-connected devices, including medical, industrial, and smart home management systems. Attackers may take over the device, take advantage of confidential information, or utilize it to carry out other unlawful acts. The biggest businesses in this industry are aware of this issue and are making efforts to enhance privacy protection for IoT device users by encrypting data and putting strong access controls in place. The advancement of artificial intelligence (AI), which can identify dangers like malware and other harmful activity in real time, also holds enormous promise for enhancing IoT device security. Nevertheless, to guarantee cybersecurity, users themselves must also be vigilant and consistently take preventive measures by setting up data protection strategies.

Keywords: Internet of Things (IoT), Cybersecurity, Cybercriminals.

[1] The paper presents findings of a study developed as a part of the research project “Serbia and challenges in international relations in 2024”, financed by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, and conducted by Institute of International Politics and Economics, Belgrade during year 2024.

INTRODUCTION

A network of physical items is known as the Internet of Things (IOT). The internet is no longer just a network of computers, it has grown to be a network of all kinds of devices, including smart phones, cars, medical equipment, toys, cameras, industrial systems, buildings, people, and animals. These devices communicate and share information according to predetermined protocols, enabling clever reorganizations, positioning, tracing, safety and control, and even personal real-time online monitoring, online upgrades, process control, and administration (Vermesan & Friess, 2014).

IoT is predicted to continue to transform our environment in the years to come, with 30.9 billion connected devices by 2025 (Cavanaugh, 2023). Also, it is anticipated that the worldwide IoT market will reach a valuation of approximately 445.3 billion US dollars in 2025 and surpass 934 billion US dollars in 2033, tripling its revenue in a decade (Vailshery, 2024a). However, the growing Internet of Things (IoT) is thought to represent the next generation of the internet, making it an appealing target for hackers (Li et al., 2014). Any connected device in the Internet of Things could potentially provide access to personal data or the IoT infrastructure (Roe, 2014). Safety demands that IoT devices be secured, particularly when it comes to medical and industrial IoT. Still, managing these devices can be challenging because they operate independently of standard network monitoring, can be purchased in huge quantities from various vendors, and may produce large amounts of data (Darktrace, 2024).

The dark web has developed into a shadowy black market where illegal activity thrives in the shadow of anonymity. Its limited accessibility reveals a decentralized structure with lax implementation of security measures, transforming it into a common hub for harmful activity. Because of the interconnectedness and vulnerability of its gadgets, the IoT has drawn the attention of cybercriminals operating off of the dark web. An IoT device that has been compromised can be the weak link that jeopardizes the security of the entire network. A compromised device can cause severe financial consequences, including ransom demands, regulatory fines, reputational damage, and remedial costs (Hodes, 2024). Based on these observations, it is clear that in order to increase user trust in IoT, accelerate its adoption, and generate new value across its verticals, and ultimately create a fully interconnected IoT environment, a radical change in the design philosophy of IoT solutions and a comprehensive convergence of IoT and cybersecurity functionalities are required (Caso et al., 2023).

LITERATURE REVIEW

Currently, efficiency and simplicity are the two main tendencies of modern man. New media is emerging as a technology that will nearly instantaneously satisfy the requirement for specific information and has facilitated speedier worldwide communication (Baltezarević & Baltezarević, 2019). Through the integration

of intelligent objects, and social and mobile networks, the Internet of Things (IoT) extends the internet and offers customers better services and applications (Yuan Jie et al., 2014).

The network of physical devices is the usual definition of the Internet of Things. Along with computers, the internet has grown to include a vast array of other devices, including smart phones, cars, toys, medical equipment, industrial systems, cameras, and even people and buildings. These devices are all connected to each other and exchange information according to predetermined protocols, which enables intelligent reorganization, tracking, and tracing as well as personal real-time online monitoring, process control, and administration (Stankovic, 2014). According to IoT terminology, a device must have these four qualities in order to be referred to as a "thing": a) The device must be able to gather and send data: IoT devices must be able to operate in settings where data can be gathered and delivered to the internet or another device. b) The devices need to be able to respond to events on its own: IoT devices can be configured to take specific actions in response to predetermined scenarios. c) The devices need to be able to accept data: IoT gadgets need to be able to get data from networks. d) Communication support: IoT devices need to be a part of a network of devices that can connect to and exchange data with one another (Palma et al., 2014).

Applications for the Internet of Things are practically ubiquitous, spanning industries and the human body. These include, among other things: 1) Health and fitness gadget sensors, including those in implantable, wearable, and countertop gadgets. 2) Automobile sensors (black boxes). Massive volumes of data regarding the behaviour of drivers and their vehicles can be gathered by these sensors. 3) Sensors for the home and grid, like smart grid and smart home systems. 4) Employees' sensors: employers can keep an eye on their staff members at work thanks to these sensors. 5) Smartphone sensors: these can be used to track a phone's movement in space, detect physical orientation etc. (Peppet, 2014).

IoT has also demonstrated its significance and promise for a developing region's industrial and economic development. It is regarded as a revolutionary move in the trading and stock exchange markets. Nonetheless, data and information security are a serious problem that requires a lot of work and is something that should be prioritized (Minoli et al, 2017). Additionally, IoT researchers and developers are actively working to improve the quality of life for the elderly and disabled. IoT has performed remarkably well in this field and given such people's daily lives a new direction. The majority of people are using these gadgets and equipment since they are easily accessible and within a regular price range, making them extremely cost-effective in terms of development costs (Gaona-Garcia et al., 2017). Neuroscience and the Internet of Things (IoT) are two quickly developing fields that are revolutionizing the healthcare sector. The integration of these two disciplines holds promise for transforming the current approaches to neurological disease diagnosis,

treatment, and prevention (Abdoullaev, 2024). Nevertheless, the findings of the initial studies in this subject are highly promising, and the application of these techniques yields remarkable outcomes. In any event, the field of neuroscience is still lacking in significant research (Baltezarević & Baltezarević, 2022).

One of the newest IoT application areas that includes smart homes is smart cities. In order to optimize comfort, security, and energy efficiency, a smart home comprises Internet of Things (IoT)-enabled appliances, televisions, streaming music and video devices, air conditioning, heating, and security systems that communicate with one another. The notion of a smart city has grown in acceptance over the past ten years, sparking a plethora of research endeavours (Zanella et al., 2014). It is predicted that by 2030, there will be over 32.1 billion IoT devices globally, nearly doubling from 15.9 billion in 2023. China will have the greatest number of IoT devices in 2033 (8 billion). IoT devices are employed in consumer markets and various kinds of business verticals (Vailshery, 2024b).

IoT is predicted to have both beneficial and negative effects on modern life, as is the case with many technologies. On the plus side, proponents of the IoT assert that it represents the first genuine evolution of the internet and that it can improve people's lives in a variety of ways, including employment, entertainment, and education (Niewolny, 2013). The communication area has become the focus of human existence. This makes it crucial how and with whom we communicate, as well as how we select, process, interpret, and use the information that we do get (Milovanović et al., 2018). However, threats to privacy and security rank among the most troubling issues with IoT. Data volumes increase by 50–60% annually in the IoT context due to the massive amount of data generated by sensors, semiconductors, smart phones, and other devices (Greengard, 2015). Security, encompassing communication networks, applications, sensing infrastructure, and overall system security, is one of the biggest challenges facing the Internet of Things (Keoh et al., 2014). Another obstacle that can diminish the benefits of IoT and hinder its adoption is technical issues. The development of IPv6 (the next generation Internet Protocol (IP)), and established management standards are critical to the Internet of Things' advancement. There is a genuine concern that those who use technology frequently may get dependent on it. Therefore, the economy sector and society at large may suffer greatly if the technology infrastructure failed for any reason, hacking, design flaws, material problems, sabotage, overloading, natural catastrophes, or crises (Onn, 2005).

It is therefore imperative that states enact more precise legislation and appropriately identify and penalize those who engage in criminal cyber activity (Baltezarević & Baltezarević, 2021). It is crucial to have the right legal and technological foundation. Analysts must fully comprehend the dangers connected to different IoT scenarios, like air travel, which involves a number of interconnected components, such as economy, safety,

and privacy, in order to establish it (Daskala, 2010). Security and privacy are significant IoT issues that need to be addressed and thoroughly researched. Consequently, in order to gain an extra edge, a private company using IoT needs to integrate data authentication, access control, attack resistance, and customer privacy into their operations. To identify global security and privacy challenges, IoT developers need to consider the geographical constraints of various nations. In order to meet the demands of privacy and security around the world, a generic framework must be created. It is strongly advised that, prior to creating a fully functional IoT framework, the concerns and difficulties surrounding privacy and security be thoroughly examined (Weber, 2010).

The variety and sophistication of threats are always changing at a rapid pace, ranging from privacy violations and data breaches to the development of powerful botnets (short for "robot network") and sophisticated malware attacks (Ray et al., 2018). Enrolling compromised devices into botnets allows for large-scale attacks that can result in distributed denial-of-service (DDoS) issues and data theft. IoT devices can become inoperable and impair vital services due to denial-of-service (DoS) assaults if they are not properly secured (Roman et al., 2011). Vulnerabilities in communication protocols and encryption techniques leave IoT devices vulnerable to illegal access and eavesdropping. These flaws can be used by hostile actors to intercept confidential data or inserted harmful commands. Attackers have opportunities to add malicious components or undermine device integrity during production because of the intricate supply chains involved in the manufacturing of IoT devices. Such weaknesses may result in pervasive breaches of security (Al-Fuqaha et al., 2015).

Nonetheless, there are causes for hope. Executives in the cybersecurity and Internet of Things domains are becoming more conscious of the problems and are actively working on solutions. Leading cloud service providers, including Google, Microsoft, and Amazon Web Services, have intensified their efforts to secure the Internet of Things. Security is increasingly given top priority in IoT architectures and hardware by semiconductor companies (like Intel and Qualcomm Technologies), whose products power important IoT devices and networks. Security is important, and pure-play IoT technology companies like Cisco Systems and Samsara offer specific IoT security solutions (Caso et al., 2023). Artificial intelligence (AI) has surfaced as a potentially effective method for tackling the problems associated with Internet of Things cybersecurity. Numerous researches have demonstrated how AI, in particular machine learning algorithms, may be used to identify and reduce cybersecurity risks in IoT contexts. Large volumes of data from IoT devices can be analysed, trends can be found, and possible attacks can be proactively countered with AI-based solutions. Subsequent studies in this field ought to concentrate on optimizing AI algorithms, investigating group learning strategies, and putting in place real-time adaptive cybersecurity systems (Djenna et al., 2021).

CONCLUSION

People may live more productive and efficient lives than ever before because to the ongoing improvements in IoT technology and its promise to potential customers to improve everyday lives, spur innovation, and revolutionize industries. Still, it is quite obvious that there is a balance to be struck when it comes to the Internet of Things (IoT) between the obvious benefits and the unforeseen consequences of living in a world full of constantly connected devices.

The readily apparent advantages of IoT that enhance our everyday lives (such as creative business models, increased productivity, and enhanced quality of life) are getting better every day. However, it is impossible to overlook the difficulties that come with the advantages, such as interoperability problems, security threats, and privacy concerns. Even while top cloud service providers have stepped up their efforts to safeguard the Internet of Things, IoT users also need to take accountability for their cybersecurity by managing their passwords, updating device firmware, and staying away from dubious links and downloads. Regular network traffic monitoring and analysis can assist in identifying any odd behaviour and reducing potential dangers before they become more serious.

Establishing thorough policies and rules for IoT security standards requires cooperation between governmental organizations, business executives, and end users. Together, they can encourage innovation in the creation of secure devices and raise knowledge of recommended practices. The assessment of the literature also emphasized artificial intelligence's potential as a useful tool for improving IoT cybersecurity. Conventional security measures might not be enough to fend off sophisticated attacks as the IoT ecosystem gets larger and more complicated.

LITERATURE

Abdoullaev, A. (2024). Combining Neuroscience and IoT in Healthcare. Retrieved from: https://www.bbntimes.com/science/combining-neuroscience-and-iot-in-healthcare (Accessed: 08.10.2024.)

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

Baltezarević, I. & Baltezarević, R. (2019). Prikriveno oglašavanje u novim medijima, Baština, sv. 48, pp. 171-179. UDK 659.1 doi: 10.5937/bastina1948171B

Baltezarević, R. & Baltezarević, V. (2022). The influence of digital political communication supported by neuromarketing methods on consumer perception towards a tourist destination. *Megatrend revija,* Vol. 19, No 2, 2022: 13-34. DOI: 10.5937/MegRev2202013B

Baltezarević, I. & Baltezarević, R. (2021). Sajber bezbednost: izgradnja digitalnog poverenja, *Megatrend Revija*, Vol. 18 (4). pp. 269-280. DOI: 10.5937/MegRev2104269B

Caso, J., Cole, Z., Patel, M. & Zhu, W. (2023). Cybersecurity for the IoT: How trust can unlock value. Retrieved from: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/cybersecurity-for-the-iot-how-trust-can-unlock-value (Accessed: 11.10.2024.)

Cavanaugh, S. (2023). IoT Cybersecurity: How Your Organization Can Tame the Wild West. Retrieved from: https://www.bitsight.com/blog/iot-cybersecurity (Accessed: 08.10.2024.)

Darktrace (2024). What is IoT Cyber Security? Retrieved from: https://darktrace.com/cyber-ai-glossary/iot-cyber-security (Accessed: 10.10.2024.)

Daskala, B. ed. (2010). Flying 2.0—Enabling Automated Air Travel by Identifying and Addressing the Challenges of IoT & RFID Technology, European Network and Information Security Agency. Retrieved from: www.enisa.europa.eu/media/press-releases/flying-2.0-study-of-internet-of-things-rfid-in-air-travel (Accessed: 10.10.2024.)

Djenna, A., Harous, S. & Saidouni, D.E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. Appl. Sci.,11, 4580.

Gaona-Garcia, P., Montenegro-Marin, C.E., Prieto, J.D. & Nieto, Y.V. (2017). Analysis of security mechanisms based on clusters IoT environments. Int J Interact Multimed Artif Intell. 4(3):55–60.

Greengard, S. (2015). The Internet of Things. Massachusetts Institute of Technology.

Hodes, A. (2024). How the Internet of Things (IoT) became a dark web target – and what to do about it. Retrieved from: https://www.weforum.org/agenda/2024/05/internet-of-things-dark-web-strategy-supply-value-chain/ (Accessed: 10.10.2024.)

Keoh, S., Kumar, S. & Tschofenig, H. (2014). Securing the Internet of Things: a standardization perspective, IEEE Internet of Things Journal, Vol. 1 No. 3, pp. 265-275.

Li, L., Li, S. & Zhao, S. (2014). QoS-aware scheduling of services-oriented Internet of Things, IEEE Transactions on Industrial Informatics, Vol. 10 No. 2, pp. 1497-1505.

Milovanović, S., Lukinović, M. & Baltezarević, R. (2018). Lični brend i integrisano marketing komuniciranje. *Megatrend revija*, Vol. 15 (1). pp. 177-186.

Minoli, D., Sohraby, K., & Kouns, J. (2017). IoT security (IoTSec) considerations, requirements, and architectures. In: Proc. 14th IEEE annual consumer communications & networking conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017. https://doi.org/10.1109/ccnc.2017.79832 71.

Niewolny, D. (2013). How the Internet of Things Is Revolutionizing Healthcare. Freescale Semiconductor, Inc. Oxford Wordpower (1999). Oxford University Press (maker).

Onn, Y. et. al. (2005). Privacy in the Digital Environment. Haifa: Haifa Center of Law & Technology.

Palma, D., Agudo, J. E., Sánchez, H., & Macías, M. M. (2014). An internet of things example: classrooms access control over near field communication. Sensors (Basel, Switzerland), 14(4). http://dx.doi.org/10.3390/s140406998

Peppet, S. R. (2014). Regulation of the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Concent. Texas Law Review, Volume, 93, Issue 1. pp 85.

Ray, P. P., De, D., & Chattopadhyay, S. (2018). Security in Internet of Things: Issues, challenges, and solutions. Journal of King Saud University-Computer and Information Sciences, 30(3), 291-317.

Roe, D. (2014). Top 5 Internet of Things security concerns. Retrieved from: www.cmswire.com/cms/internet-of-things/top-5-internet-of-things-security-concerns-026043.php (Accessed: 11.10.2024).

Roman, R., Alcaraz, C., & Lopez, J. (2011). Botnets of Things: A New Threat? Computer Networks, 55(2), 308-319.

Stankovic, J.A. (2014). Research directions for the internet of things. IEEE Internet of Things Journal, 1(1): 3-9.

Vailshery, L. S. (2024a). IoT global annual revenue 2020-2033. Retrieved from: https://www.statista.com/statistics/1194709/iot-revenue-worldwide/ (Accessed: 10.10.2024).

Vailshery, L. S. (2024b). Number of IoT connections worldwide 2022-2033. Retrieved from: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (Accessed: 09.10.2024.)

Vermesan, O. & Friess, P. (2014). Internet of Things–From Research and Innovation to Market Deployment. River publishers' series in communications.

Weber, R.H. (2010). Internet of things-new security and privacy challenges. Comput Law Secur Rev. 26(1):23–30.

Yuan Jie, F., Yue Hong, Y., Li Da, X., Yan, Z. and Fan, W. (2014). IoT-based smart rehabilitation system, IEEE Transactions on Industrial Informatics, Vol. 10 No. 2, pp. 1568-1577.

Zanella, A., Bui, N., Castellani, A., Vangelista, L. & Zorgi M. (2014). Internet of things for smart cities. IEEE IoT-J.1(1):22–32.