Analysis of IoT Devices Security for Household Applications

M. Milenković, R. Nikolić, S. Čelan, P. Petrošanec
University of Zagreb, Faculty of Transport and Traffic Sciences/Chair of Transport Law and Economics, Zagreb, Croatia
mmilenkovic@fpz.unizg.hr

Abstract - According to predictions that the world consumption of Internet of Things (IoT) devices will exceed 772 billion dollars this year and considering the increasing spread of IoT devices and the number of investments in them, the paper will present the authors' view on the security of IoT devices. The paper is based on the conducted research through a quantitative analysis of the familiarity and safety of the use of IoT devices in the household. The paper intends to diagnose the growing potential risks that could threaten the security of IoT households across the EU. As one of the instruments for the protection of end users, the paper will instruct legislators on the minimum technical and security requirements IoT devices should use for end users to have more protection, and security in the rapidly growing category of household devices. The security of IoT devices will be analyzed based on the known attacks on IoT devices and the survey conducted among the population of citizens of the Republic of Croatia. *De lege ferenda*, legislators will be called upon to define the minimum "reasonable" security features that should become part of all IoT devices sold in the EU by 2030.

The key words: IoT devices, security, cybersecurity, data protection, household application.

I. INTRODUCTION

This paper continues the research on the security of IoT devices, which was conducted through a questionnaire among the adult population of the citizens of the Republic of Croatia (further: Croatia). All adults in Croatia who participated in the questionnaire had the opportunity to answer the questions regardless of their age and/or gender.

504 respondents participated in the research intending to analyze their awareness of IoT devices' possibilities. The majority of respondents (56.6%) believe that IoT devices and their use do not contribute (or contribute in a minor percentage) to improvements to the quality of their life. Furthermore, 2.9% of respondents replayed that their data is not exposed to potential threats on the Internet, while 56.4% answered that their data is somewhat exposed to threats, and 40.7% are aware of the dangers that can happen with their personal data on the Internet. [1] From the respondents' answers in the questionnaire, it can be concluded that citizens are not familiar with the operation and abilities of IoT devices and that they are not aware of the dangers to their personal data. It is important to note that the respondents are aware of the inadequate involvement of the system in terms of education and weak regulation, as well as insufficient information on the part of the manufacturers. From the previous can be concluded there is a need to improve the legal framework and education regarding awareness and protection of the personal data of end users.

Based on the mentioned research, the authors wanted to raise the level of awareness of the end users and propose the implementation of education in primary and secondary schools with an emphasis on higher education institutions in the field of technical professions. Previous also includes lifelong education of older citizens and also all the other citizens outside the schooling system.

In this paper, the authors review the security of IoT devices based on the research of recent literature, the previously mentioned questionnaire and the personal use of various small-scale devices.

Therefore, the aim of the paper is to present a realistic picture of the entire system and the potential and ubiquitous dangers to which this technology exposes end users, their households and their personal data.

II. ADVANTAGES AND DISADVANTAGES OF IOT DEVICES IN THE HOUSEHOLD

A. Literature review

Various authors [2] [3] [4] point out that IoT devices have more advantages than disadvantages, and some of the most important ones are listed below. Among the authors mentioned, *minimisation of human effort* stands out as the main advantage of IoT devices as they reduce the need for human intervention by communicating and connecting with each other and performing various tasks without human intervention.[3]

Some of the benefits also cited by the authors include *smart home systems* that are connected to the internet 24/7, *home automation systems and reliable energy management systems*. [5]

In addition, [6] states that the IoT allows users to *access information in real-time* from anywhere in the world. ‘’Users can connect to the app and collect data about their personal devices whenever they are able to connect to the Internet. One of the main benefits of IoT integration is that processes become more adaptive to what is actually happening in the real world. Inherently, this is based on events that are either detected directly or by real-time analysis of sensor data.’’

Also, *patient care* can be delivered more efficiently in real-time without the need for a doctor's visit. It gives them the ability to make decisions and provide evidence-based care, which is called Smart Health System [4]. It includes

smart devices and appliances that support human health, reduce medical costs and even shorten hospital stays. Such devices can be used to check and monitor various health problems and even fitness levels or the number of calories burned. They are also used to monitor critical medical conditions in hospitals and trauma centres.

The Internet of Things has changed the entire environment of the medical field by facilitating it with smart devices. [7] [8].

Another important aspect of peoples' lives is transportation, where the IoT is bringing significant improvements. Vehicles available in the market are equipped with pre-installed sensor devices that are interconnected and can predict and suggest routes taking into account the real-time traffic situation on the road (e.g., fleet tracking). The exciting things that the IoT offers today is the ability to pre-order a charging station for electric cars. [9] [6].

On the other hand, the disadvantages of IoT technology in homes, according to most authors, are as numerous:

First of all, users' data becomes accessible, and hackers can tap sensitive information. A data breach usually occurs when a third party (usually an attacker) can access the user's data without the user's knowledge and awareness. And this data can ultimately be used to manipulate the user, i.e., to manipulate their smart home devices.

Security, and thus privacy, are significantly threatened because IoT systems are connected to numerous devices that communicate within the network. This would mean that there is little to no privacy between the devices on the network and that data is exchanged to make the devices more efficient. IoT devices are more vulnerable to security threats and attacks due to weak technical quality standards.

Currently, there is a lack of adequate security solutions for IoT devices and applications that "lead the world of securely connected things towards the Internet of insecure things". [10] It is therefore necessary to pay attention to security threats and the resulting privacy issues.

B AUTHORS' VIEW

Based on the questionnaire mentioned, research of current literature and independent use of IoT technology in their households, the authors list the following main advantages and disadvantages of IoT devices, according to their own experience. Some of the main advantages of IoT devices that are relevant to the daily lives of smart home users are:

a.) the automation of activities, which reduces the time needed to perform certain actions in the household, usually via a smart home application. For example, the user of a smart home can remotely turn on the heating and cooling system remotely, in advance, and set the temperature in the smart home, also the oven in the smart home can be set in advance to have a ready meal when arriving at the household For example, there is also the possibility to unlock the house/flat via a mobile application to let the handyman in, without coming back home; it can also be done remotely;

b.) healthcare for patients can be significantly improved through the application of telemedicine. With the help of software and digital solutions, servers and IT equipment should be offered, staff trained and the basis for telehealth strengthened, which would enable disadvantaged groups in particular to access medical care (remote patient monitoring). This also includes elderly and frail citizens who can stay in their homes without having to go to old people's and nursing homes;

c.) simplification of traffic flows and smart traffic signals - the user of a smart household can check the fastest way home through the smart-home application and pre-set the opening time of the garage door;

d.) availability of information at any time - for example, a student living in a smart home can search the online library and study materials needed from home, and employees can also do their work remotely.

On the other hand, some of the disadvantages brought by connected IoT devices in the smart household are:

a.) loss of privacy and loss of data privacy, i.e., the availability of all data via the household's smart network via connected IoT devices, the user's personal and intimate data become available to attackers who would want to threaten such a household in any way;

b.) the danger of complete loss of control - the possibility of interruption for using the application for controlling the system of a smart (connected) household - blocking of IoT-connected devices by a third party, usually intruders, i.e., attackers, e.g., complete blocking of the system and unauthorized access to the household;

c.) misuse of connected devices in the household - a third party controls and downloads personal data via connected devices without the permission of the household owner and sells personal data, i.e., shares data with third parties, which can afterwards be used for marketing or any other not permitted purposes;

d.) low system features – end users have no control and often get a simplified interface, which limits the mitigation of vulnerable services. Accordingly, end users have almost no control or insight into the operation of the IoT household devices.[11]

On the one hand, we list the above benefits because the primary function of IoT devices is to improve the lives of the users of these devices and technologies that improve the lives of the general population, as the example of the use of IoT in the healthcare sector shows.

On the other hand, such devices are full of flaws that manifest themselves in the loss, disclosure and sale of personal data of end users without their knowledge to third parties where it is not specified who third parties are.

Therefore, one of the priorities is to propose a privacy standard that would decisively cover the obligations of

TABLE 1: Display of criteria that privacy policies of IoT device manufacturers meet *according to GDPR*

Criteria	Samsung	Google	AWAIR	Honeywell
Sharing of data with third parties without consent of end users	X	X	/X	/X
The possibility to change data by end users (editing, deleting, sharing, downloading)	/X		/X	/X
Right to erasure ('right to be forgotten')	X	X	X	X
Lack of regulation				

manufacturers and sellers of IoT devices. It will be further explained in chapter IV and chapter V.

All data from Table 1 are the results of the Privacy policies of the companies mentioned in this paper Samsung [12], Google [13], AWAIR [14], and Honeywell [15].

The companies in Table 1 are at the same time manufacturers and sellers of IoT devices and were therefore selected to be ranked in this comparison. The results from Table 1 show that the major manufacturers of IoT devices do not apply the GDPR regulations in full, which is evident from their privacy policies. Therefore, the companies that occupy a large part of the internal market of EU Member States are unintentionally putting end users personal data at risk. Their privacy policies are not transparent and easily readable to the average end user; on the other hand, they are complex and complicated to read even to experienced users.

Although Article 8 of Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights [16] provides the consumer with such information in plain and intelligible language, in a manner appropriate to the means of distance communication, and where such information is provided on a durable medium, it must be legible.

Under Article 17 of the GDPR, the data subject should have the right to rectification of personal data and the "right to be forgotten" where the storage of such data infringes the Regulation or the law of the EU or of a Member State to which the controller is subject.

The data subject should have the right to have his or her personal data erased and no longer processed if the personal data are no longer necessary for the purposes for which they were collected or otherwise processed.

Likewise, where the data subject has withdrawn consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data is otherwise not in compliance with the Regulation. [17]

The results of the privacy policies show that manufacturers avoid the provisions of the GDPR, i.e., they do not apply them entirely which is also visible from the Table 1 rationale.

Accordingly, it is clear that manufacturers do not inform end users about the sharing of their data nor about the capabilities of IoT devices, and for the mentioned reasons there are frequent breaches in IoT systems and the loss of personal data of end users, whose initial protection is mandated by the GDPR.

III. STATISTICAL DATA ON ATTACKS AND SECURITY OF IOT DEVICES

According to EUROSTAT statistics for 2022, the countries with the highest percentage of users who own IoT devices in their household (e.g., alarm systems, smoke detection systems, surveillance cameras, door locks or other internet-connected security-safety solutions for home) are Norway (24.37%), the Netherlands (22. 68%), Sweden (18.23%), Denmark (16.61%), Ireland (15.96%) and Estonia (15.72%). The Republic of Croatia is in 23rd place with 5.87% of users [18].

It is significant to point out that there is a certain lack of reliability among EU citizens that this technology brings with it. This is evident from statistical data, which shows that the percentage of users concerned about the security of IoT devices is higher than the percentage of users who own these devices.

Austria is the leading European country when it comes to the percentage of users who are concerned about security with 27.13% of users. It is followed by Finland with 23.36% of users, while Croatia is third with 20.39%. This claim can also be supported by the fact that in the countries mentioned, an even higher percentage of users are concerned about the privacy and security of the personal data generated by such devices. For Austria this percentage is 28.50%, for Finland 24.16% and for Croatia 21.10% [19].

This could indicate two possibilities:

a) citizens are not sufficiently familiar with technology, and/or

b) citizens are familiar with technology and are aware of the potential dangers such devices can cause. Based on the questionnaire conducted for the purpose of researching the awareness of the citizens of Croatia about the possibilities of IoT devices, it can be concluded that the citizens are not sufficiently familiar with IoT technology but are also aware of the shortcomings of the entire system. From above is evident that a large number of EU citizens do not trust the security of IoT devices.

It is important to note; when purchasing an IoT device, end users do not sign the consent for sharing of their data,

which is prescribed by the GDPR. [20] While when purchasing an IoT product, end users should always sign a consent form that lists all the potential risks the user is taking on by purchasing such a product and specifies the warranty period, i.e., the period until which the vendor commits to provide software support and security patches to each user. This is explained in more detail in the next chapter. It is also important to mention that in the last ten years, there have been a few significant attacks on IoT devices.

Such attacks have shown how vulnerable the IoT device network is and how easily breakable to steal the data stored by the device or even to block the entire system.

One of the largest IoT attacks in the history of IoT was the Mirai botnet, which occurred in October 2016 and infected over 600,000 IoT devices. [21]

The scale of the threat posed by IoT devices can also be seen in the example of the attack on Jeep and Tesla automated cars.

In 2015, there was a company-initiated "attack" on Jeep Cherokee vehicles that identified steering wheel vulnerabilities. In this planned presentation of a possible attack, it was found that it was possible to remotely control a car and 1.4 million cars of the said brand were taken out of circulation. [22]

This suggests how common attacks on IoT devices of all profiles have become.

In some cases, users cannot even tell that their devices are being monitored, i.e., that their personal data is being shared, and even if they find out, they still do not know with which third parties their data have been shared and to what extent.

IV. HOW TO REGULATE LEGAL FRAMEWORK AND PROTECT END USERS?

Nowadays, most governments consider data protection as a basic human right [23] but in practice it looks different.

However, existing privacy laws and regulations are not specific to IoT devices. We argue that they are insufficient to recognize important differences between general privacy scenarios and IoT-specific scenarios. [24]

The European general data protection framework includes the GDPR [20] but it does not explicitly mention IoT devices.

Neither Croatian national law; nor the Croatian Act on the Implementation of the General Data Protection Regulation [20] does not contain any statements and provisions applicable to the collection of data via smart home devices and the Internet of Things, and none of them specifies what happens to personal data and/or special types of personal data and with whom they are shared and for what purposes. IoT products and services enable the collection of large amounts of data, some of which as specific types of personal data can be potentially sensitive. Therefore, it is necessary to take protective measures without jeopardizing the users' privacy.

Recital 4 of the GDPR sets out the basic principles of the Regulation. It states that "the processing of personal data should be lawful, fair, and transparent to the data subject."

The GDPR [9] requires that the service provider ensures the safety and security of the processing. It considers this further in the introductory statement 39, elaborating the principles of data protection, especially the principles of purpose limitation, storage limitation, and data minimization: "Natural persons should be aware of the risks, rules, protective measures and rights related to the processing of personal data and how to exercise their rights related to such processing."

Manufacturers' privacy policies are usually not compatible with the obligation of the EU to provide for a high level of consumer protection, as mentioned in Article 169 [25] of the Treaty of the Functioning of the European Union.

For this reason, it would be necessary to oblige manufacturers and sellers to respect privacy standards. Privacy policies should include:

- a list of what kind of personal data manufacturers and vendors collect, maintain, or share,
- notifications for the end users about their data privacy,
- a reasonable consent consisting of risks IoT technology brings with all details not defined by default in the security standards,
- a guide for end users' access to download and edit their data,
- organizations and third parties the personal data are shared with, and their conditions. [26]

Specifically for Croatia, it would be necessary to adopt a regulatory privacy standard that obliges producers and vendors to have users' consent when selling IoT devices to end users.

Consent should be written in clear, comprehensible, and simple language; in terms of IoT device capabilities and by signing the consent the user accepts all given risks.

The authors consider these as minimal "reasonable" security features that should become part of all IoT devices sold in the EU in the next decade. This is currently not regulated by the GDPR nor any other Act of the *Acquis*. Updating IoT devices should not be left to chance. Privacy and security requirements will have to be implemented in the original design process of the device, network or storage system and GDPR will have to adapt accordingly.

Why is it necessary to adopt tougher criteria for producers?

Precisely because it is necessary to bring a higher level of product security with digital elements, which will ultimately increase user confidence in these products.

Vendors, on the other hand, should be responsible for keeping devices up to date.

IV. CONLUSION

The IoT spans a variety of industries, including healthcare, transportation, the consumer rights sector and

the private homes of end users. Even when the attack occurs, the average citizen might not be aware that any IoT device can be compromised. Cybersecurity is everyone's responsibility and an important issue for everyone, not just businesses.

The large number of devices connected to the internet produce enormous amounts of data. This is ultimately the biggest challenge in the IoT sector, as it is most difficult to secure IoT devices and the data exchanged over the network. As end users' private data is transferred between devices, various security challenges such as privacy, confidentiality, integrity and reliability need to be addressed.

It is also crucial for a large number of end users, as according to Statista [27] [28], the number of smart home users in Europe was estimated to reach 64.7 million people in 2022, and how much will the number of users grow in the next 5 years?

Therefore, data security is a key issue for all sectors, especially for households where a large amount of personal data is stored.

One of the aims of this paper was to highlight the current state of IoT device security, the transparency of IoT device manufacturers and vendors to end users, and give an insight into their privacy policies.

The authors proposed the key points of a data protection standard they believe should be mandatory for all manufacturers and vendors of IoT devices in EU member states.

They also pointed out that the privacy policies of individual IoT device manufacturers are not in line with the provisions of the GDPR and Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights [16], nor is the end user support system, which should be simple, transparent and easy to understand according to the legal framework mentioned in this paper.

As a result, the system of networked IoT devices in the smart home is exposed to dangers and risks that end users are not even aware of. This is evident from the statistical data in Chapter 3 for EU countries.

For this reason, their homes and their personal data are exposed to daily use by manufacturers, their partners and third parties who are not clear about who they are and under what conditions they process end users' data.

The General Data Protection Regulation does not oblige manufacturers as much as it should, given the number of IoT devices in households representing a large part of the market. On the one hand, the Regulation needs to be completed as it has not been amended or supplemented since its adoption, and on the other hand, the market is changing rapidly.

Therefore, the authors propose a more detailed check of compliance with the GDPR and, as far as the market for IoT services is concerned, to regulate this area more strictly in the manner written in this paper.

REFERENCES

[1] P. Petrošanec, S. Čelan, R. Nikolić, M. Milenković, Awareness of Croatian citizens about the advantages and disadvantages of IoT devices and their safety, MIPRO proceedings 2023, [Manuscript accepted and submitted for publication in MIPRO proceedings 2023]

[2] Aplus Topper, What is IoT? Advantages and Disadvantages of Internet of Things (IoT), 2022, https://www.aplustopper.com/advantages-and-disadvantages-of-iot/#Advantages_of_IoT, [Accessed 9th of March 2023]

[3] TechVidvan Advantages and Disadvantages of IoT, https://techvidvan.com/tutorials/advantages-and-disadvantages-of-iot/, [Accessed 9th of March 2023]

[4] Kumar, S., Tiwari. P., and Zymbler., M., ''Internet of Things is a revolutionary approach for future technology enhancement: a review'', Journal of Big Data, (2019) 6:111, https://doi.org/10.1186/s40537-019-0268-2, pp. 2-3., https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0268-2#Ack1, [Accessed 9th of March 2023]

[5] Geeks for Geeks, Advantages and Disadvantages of IoT, 2022, https://www.geeksforgeeks.org/advantages-and-disadvantages-of-iot/, [Accessed 8th of March 2023]

[6] Internet of Things From Research and Innovation to Market Deployment, 2014, River Publishers, p. 79

[7] Sfar AR, Natalizio E, Challal Y, Chtourou Z. A roadmap for security challenges in the internet of things. Digit Commun Netw. 2018;4(1):118–37.

[8] Minoli D, Sohraby K, Kouns J. 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.2017.7983271.

[9] Behrendt F. Cycling the smart and sustainable city: analyzing EC policy documents on internet of things, mobility and transport, and smart cities. Sustainability. 2019;11(3):763.

[10] Kholoud Y. Najmi, M. A. AlZain, Mehedi Masud, N.Z. Jhanjhi, Jehad Al-Amri, Mohammed Baz, A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability, Materials Today: Proceedings, 2021, Internet of Things 19 (2022) 100564, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2021.03.417., (https://www.sciencedirect.com/science/article/pii/S221478532102469X), Internet of Things 19 (2022) 100564

[11] O. Alrawi, C. Lever, M. Antonakakis and F. Monrose, "SoK: Security Evaluation of Home-Based IoT Deployments," 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019, pp. 1362-1380, doi: 10.1109/SP.2019.00013., p.5

[12] Samsung. *Samsung´s Privacy Policy*. Available: https://privacy.samsung.com/privacy/samsung [Accessed 3rd of April 2023]

[13] Google. *Privacy Policy*. Available: https://policies.google.com/privacy?hl=en-US [Accessed 3rd of April 2023]

[14] AWAIR. *Privacy Policy*. Available: https://store.getawair.com/pages/privacy-policy [Accessed 3rd of April 2023]

[15] Honeywell. *Honeywell Privacy Statement*. Available: https://www.honeywell.com/us/en/privacy-statement#english [Accessed 3rd of April 2023]

[16] Directive 2011/83/EU of the European parliament and of the Council on consumer rights, amending Council Directive 93/13/EEC and

Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32011L0083&from=EN [Accessed 29th of March 2023]

[17] The EU General Data Protection Regulation (GDPR), Oxford University Press, 2020

[18] Eurostat. *Internet of Things - use*. Available: https://ec.europa.eu/eurostat/databrowser/view/isoc_iiot_use/default/table?lang=en (Accessed 9th of March 2023)

[19] Eurostat. Internet of Things - barriers to use. Available: https://ec.europa.eu/eurostat/databrowser/view/isoc_iiot_bx/default/table?lang=en (Accessed 9th of March 2023)

[20] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, preamble 39, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=HR, [Accessed: 20th of February 2023]

[21] V. Unterfingher, A Technical Analysis of the Mirai Botnet Phenomenon, 2021, Available: https://heimdalsecurity.com/blog/mirai-botnet-phenomenon/

[22] Geenberg A. *Wired, Hackers Remotely Kill a Jeep on the Highway—With Me in It.* Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [Accessed 3th of April 2023

[23] Web Hosting Secret Revealed. *The Simple Privacy (and Cookie) Policy Guide for Website Owners.* Available: https://www.webhostingsecretrevealed.net/blog/blogging-tips/have-a-website-you-need-a-privacy-policy-heres-why/ [Accessed 3th of April 2023]

[24] A. Subahi and G. Theodorakopoulos, "Ensuring Compliance of IoT Devices with Their Privacy Policy Agreement," 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, Spain, 2018, pp. 100-107, doi: 10.1109/FiCloud.2018.00022.

[25] Consolidated version of the Treaty on the Functioning of the European Union OJ C 326. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/TXT&from=EN [Accessed 5th of April 2023]

[26] The Internet of Things, Legal Issues, Policy, and Practical Strategies, C., A., Suarez, C., H., Cwik, and L., Thomson, American Bar Association Book Publishing, 2019, pp. 25 -27

[27] Statista. *Number of smart home users in Europe in 2022.* Available: https://www.statista.com/forecasts/1283896/smart-home-users-europe-segment [Accessed 5th of April 2023]

[28] Jansen B. 60+ IoT Statistics, Facts & Trends. *vpn Alert.* Available: https://vpnalert.com/resources/iot-statistics/?gclid=EAIaIQobChMIre72h4nP_QIVQo9oCR1PAgJaEASAAEgK9xvD_BwE#IoT_Devices_Statistics [Accessed 9th of March 2023]