International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 10 – Issue 02 || Mar - Apr 2025 || PP. 01-12

The Influence of Residents' Actions on the Security of Smart Homes

Nicolae-Gabriel Vasilescu[1]
[1]*Faculty of Cybernetics, Statistics and Economic Informatics,*
Bucharest University of Economic Studies, 010552 Bucharest, Romania

Abstract: This paper presents the influence that the actions and behavior of the inhabitants have on a smart home and the main problems that may arise at the security level due to the improper use of existing devices or applications used daily. A survey was conducted among students from the Faculty of Cybernetics, Statistics and Economic Informatics, Bucharest University of Economic Studies, in their second year of the bachelor's degree, which aimed to address some topics regarding security and good practices that should be considered in everyday life. There are more and more smart devices used at home interconnected through an Internet of Things network, and their proper use has become a necessity considering the existence of many types of attacks of all kinds. There were 156 responses presented in this article, which represent the actions performed or not by the students participating in this study.

Keywords: smart home, security, IoT, inhabitants' actions

1. Introduction

The behavior of the inhabitants of a smart home is an important aspect in security management and involves a series of measures that must be considered in everyday life. There can be data leaks through various actions of manipulating the devices present in that home.

Currently, there are many applications that manage the change of states of some smart devices or installations, such as managing the heating plant, hot water, air conditioning installations and others.

An important point regarding the security level of smart homes is the use of smart devices and applications components through which the existing IoT network is managed.

This paper aims to follow the behavior of some students from the Faculty of Cybernetics, Statistics and Economic Informatics who are in the second year of the bachelor's degree, precisely to see how these people who study technology at the faculty manage and what behavior they have in relation to the devices and applications used at home.

In this survey there were 156 students, and the questions aim to track essential aspects regarding smart devices and applications, such as network use, passwords and configurations that can be set. The questions below consider the connection between devices, applications, installations and the people who use them, as well as the connection between residents and visitors, to observe whether information leaks can occur, to different types of attacks that can be carried out by any person with access to their own internet network used at home.

There are increasingly secure devices and applications on the market, with a very complex usage dictionary that many do not analyze and do not go through with much interest. Certain installation steps can be omitted that can have an essential role in security and that can give much easier access to the outside.

Using passwords with reduced complexity can lead to obtaining information from outside the home quite easily, even reaching the management or impacting the level of comfort.

Protecting personal data is the goal in mind through the proper management of the entire smart network without unauthorized access from both inside and outside.

Residents are responsible for the actions they take that can have a physical but also intellectual security impact, by voluntarily or involuntarily exposing shared data, such as passwords, or by sharing useful information in an insecure way, or for other reasons.

There are many sites that expose the vulnerabilities that may exist on different versions of applications or devices, described in detail that can greatly help residents in carrying out their household activities both inside and outside the home as securely as possible.

The high level of security enjoyed by the entire network can be impacted by residents through various ways used by possible attackers who can be of any kind.

Many users ignore security updates, which can leave devices vulnerable to cyberattacks as each new version covers certain problems from the past that have been tested and fixed by new updates.

Leaving devices permanently connected to the internet without protection or keeping default settings can increase the risk of hacking even from known people who may end up gaining unauthorized access to private data.

Regularly checking access logs and notifications of suspicious activity can prevent security incidents, in this way, unusual traffic that occurs without residents doing so intentionally can be identified.

2. Materials and Methods

A smart home is a residence that uses intelligent equipment and advanced technology to help residents in their household and leisure activities by increasing the quality of life, bringing a greater degree of automation to the processes, as presented in [1].

An Internet of Things (IoT) network refers to the interconnection of intelligent components that make up it, components that exchange data with each other without direct human involvement. In [2] this network is detailed, which is the basis of smart homes, where devices and applications communicate with each other in real time.

The survey conducted in this paper uses several types of questions that aim to obtain data that show and define human behavior in relation to devices and applications used in smart homes. The 156 responses received formed the basis for the elaboration and interpretation of the question that defines this thesis, namely the influence of residents' actions on the security level in a smart home.

The CSV file containing the survey data was sent as a request along with this paper. This study analyzes 16 questions out of a total of 22 questions that were asked to students.

It starts with identifying the types of smart devices used at home to apply different strategies and elements regarding the degree of use of the processes made available in smart homes. There are many categories on the market that have a very important role in household activities and that can facilitate different activities.

According to [3], The Common Vulnerabilities and Exposures (CVE) is a software that deals with the analysis and description of existing vulnerabilities at the level of ap-plications, devices, which receive a unique id. By accessing this software, one can quickly obtain a list of existing vulnerabilities at the level of the version used in the smart home. This aspect can be checked very easily online depending on the product used, the brand, or other characteristics of a device used.

By consulting these issues, it is very easy to see if a certain vulnerability exists, if it has been fixed or what consequences it may have on the version used.

This can be an important initial step in quantifying how secure the devices that form smart network are compared to the current period.

Knowledge of the functionalities provided by the devices and applications used is another important factor that can protect data more optimally from a security point of view when the functions that the product has are very well documented by the people who use them. In this doctoral thesis, [4], general properties are exemplified that apply to the functions that the devices used have that cover data security.

The degree of knowledge of as many functions as possible helps the user to use all the processes they open more easily and automatically, ensuring a higher level of security. Regarding data protection, if they are shared, the best ways to ensure transfer without problems, avoiding different types of attacks, are sought in the documentation.

As shown in [5], terms and conditions can influence the life cycle of applications and devices used because there may be clauses that are not in line with what the user wants to use or install.

Reading the terms and conditions is necessary before configuring any tool used in a smart home to avoid unwanted aspects of the respective product. Very often, these steps are quickly passed before installation, without being given enough time to understand exactly all the features and even problems that may exist.

Changing passwords frequently is an approach that can stop the various attacks that occur periodically and checking the passwords used first, as presented in [6], can be a solution even for the scenario when the attack has occurred, and to regain control over the account used a new password is needed before other actions that can obtain sensitive data can take place.

Both changing passwords and storing them somewhere secure, even encrypted, can significantly increase the overall security level in the smart home. Residents must have controlled access to passwords, depending on their knowledge and needs on the different smart components.

According to [7], a solution to attacks on a username and password can be password breach alerting, which shows if a combination of username and password is executed more than once to gain access.

As presented in [8], most of the time because of forgetting a certain password or fear of forgetting it, passwords are shared with family members or friends, without considering that this problem can give access to the data very easily both from inside and outside. This practice is common, and those involved never think about what another person can do with passwords at the smart home level, if that person can gain access or if they want to have access to some connections.

A possible solution to avoid password sharing is detailed in [9] and consists of using password managers to securely store all passwords used without the possibility of effectively forgetting those passwords.

The study also looked at password reuse, a factor that makes attacks with passwords used from another context to other applications/devices possible. There are many people who reuse old passwords for other tools at home, and the life cycle of a password does not end only at the level of one component, being extended to other components in the IoT network, as shown in [10].

As demonstrated in [11], there are many users who use weak passwords on the platforms or applications they use, generally forming passwords so that they are validated by the respective system as being in order. The need to use strong passwords to make it difficult for specialized attackers to obtain them is also the basis for building a hard-to-attack IoT network.

Based on [12], strong passwords can avoid or make more difficult brute-force attacks that test multiple passwords from a predefined dictionary until they find a combination of multiple words that matches the password.

There is a scenario where a user uses old passwords or adds one or more characters either on the same device or on other devices. As shown in [13], this practice is quite common, not making it difficult to obtain passwords that are quite identical in word order or character length. It is an easy way to change a password by adding extra characters, but it is a correct approach because starting from the old password is only one step away from fully identifying the final form.

Regarding the WI-FI network used in smart homes, the use of the Wi-Fi Protected Access 3 (WPA3) protocol brings security improvement through a better encryption method and key sharing, as demonstrated in [14], bringing a high degree of security for the entire network used. The attacks that stop before they reach the network, the encryption methods but also the aspects that made this protocol necessary show the utility and necessity of using it in a safe network.

Two-Factor Authentication (2FA) is another solution to increase the security of applications and smart devices used by residents, and in the paper [15], it is shown that this option adds an additional step to the tasks but also increases the complexity of the possible attacks that can occur. It is an extra layer of security that can prove very useful.

Starting from [16], the use of secure channels to communicate data both within the IoT network, but also from/to the outside brings another plus in terms of the complexity and security of the smart home, so that any kind of information transfer is encrypted and secure.

In a continuous emergence, security threats are becoming more and more present in an era of highly advanced technology, followed by solutions that fix them as presented in [17]. It is important to know the existing problems since the respective version is used at home on different components in the network, to identify if there is a possibility that it in-fluences to some extent the daily process that is being carried out.

Using a single network in a smart home can also bring benefits, and as explained in [18], there can be multiple sensors or multiple components communicating within a network, but it can also bring disadvantages, in the case of attacks the entire network is accessible in some situations.

As shown in [19], reputable brands are the most trustworthy from many points of view because they have been tested on several customers and there is a good degree of satisfaction obtained over the years.

There is security guarantees offered and even support in case of various questions or ambiguities encountered regarding the components used in the smart home.

To resolve issues that are underlying older versions used, there is the possibility of periodic updates regarding the applications or operating systems used. These updates fix certain problems described and documented to be public.

The acceptance and use of the smart home is a rather complex topic, as can be seen in [20], which brings benefits in terms of quality of life and ease of tasks performed, but where there may be various problems if the components are not used properly in the IoT network.

3. Results

The questions asked aim to observe the actions taken by the inhabitants of smart homes and their impact on the degree of security both at the device level and at the level of the entire IoT network. Even those highly secured systems, by not following some steps and very strict regulations, can lead to unauthorized access to their own network, to leaks of sensitive information, but also to other states that may occur.

The study began by identifying the types of smart devices used at home. The most used devices are smartphones, smart TVs, smartwatches, and smart lights.

As shown in Figure 1, all survey participants use at least one smart device at home that falls into different categories, so future questions will address different topics related to different security topics regarding the various applications and devices used at home.

In the age of technology, all processes are automated, making daily activities easier, sometimes without the need for physical human presence.

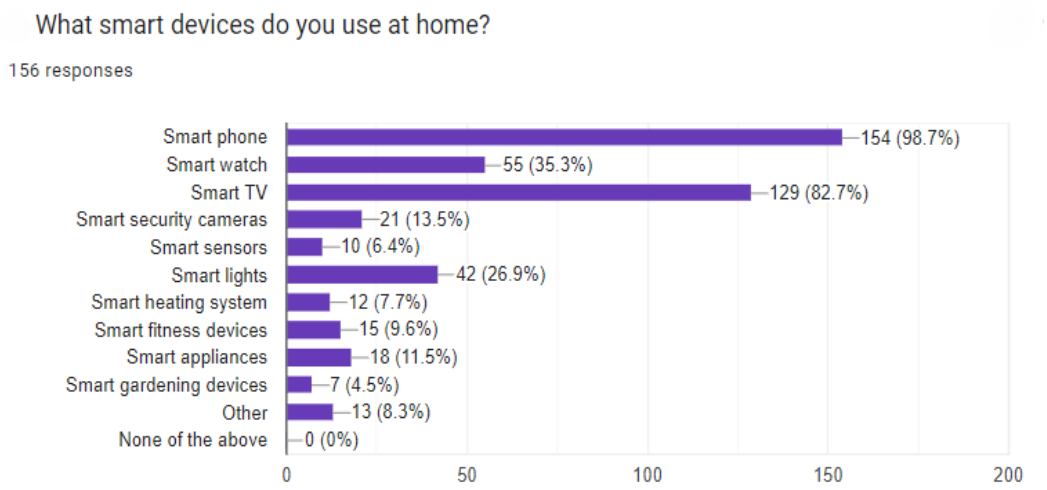

Figure 1: Smart devices used at home.

To check if the applications or devices used in a smart home have certain vulnerabilities, there is the possibility of additional checks performed by querying Common Vulnerabilities and Exposures (CVE). This database shows whether a specific product, according to certain filters, has certain vulnerabilities for certain vulnerabilities. You can identify the versions that fix the problems, the dates on which they were fixed and other important details.

In Figure 2 below, most of the responses indicate that this vulnerability database is not used that much, with the most common being sometimes. It is also noteworthy that over 40 respondents said that they have never accessed this database.

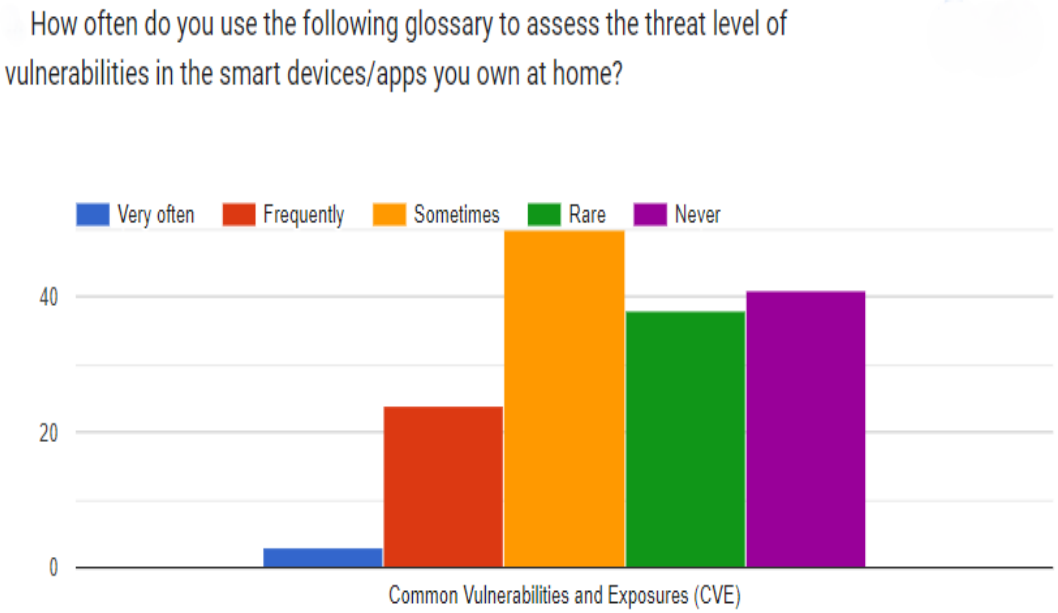

Figure 2: CVE usage for smart devices.

Another interesting aspect is about the functionalities of the products or applications used which, in addition to facilitating certain processes that can be automated, can increase the security level of the smart home through proper use. The more functions of the products used are known, the more their use increases the security of the entire IoT network.

Figure 3 shows that more than half of the respondents know most of the existing functionalities and underlying devices or applications used at home. A very small percentage do not know any functionality of the products used, there are quite a few answers that show that they are partially aware of the existing functions.

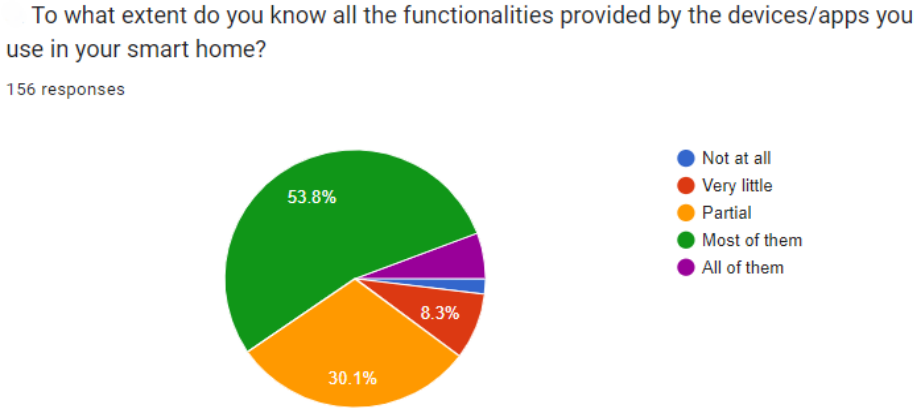

Figure 3: Functionalities provided by devices/applications

Regarding the terms and conditions, from figure 4 it can be seen that a very high percentage of respondents are not careful when installing an application. Very few read the terms and conditions carefully. This aspect can lead to the emergence of various data security problems, because in that document certain things can be exposed that contradict the needs of the customers and that contrast with the expectations they had.

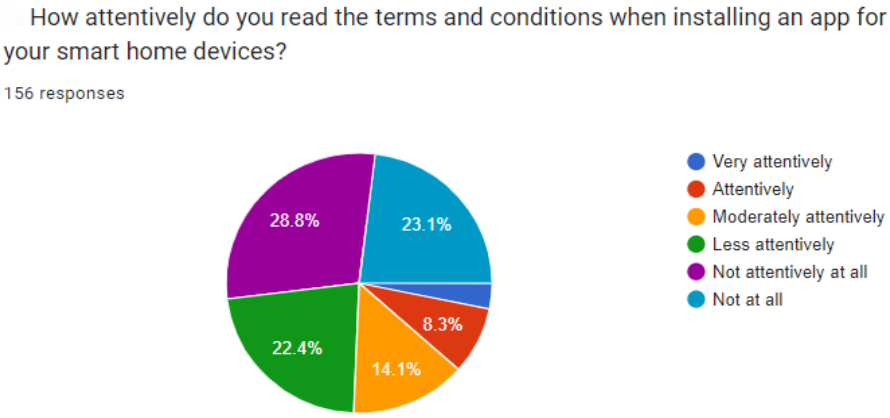

Figure 4: Terms and conditions

The topic of passwords is one of the most important because they give access to smart devices and applications, making a secure network potentially vulnerable if pass-word management is questionable. In figure 5, more than half of the respondents change their passwords rarely, which makes possible attacks have a higher chance of success. A small percentage change their passwords, and approximately 10% never change their passwords.

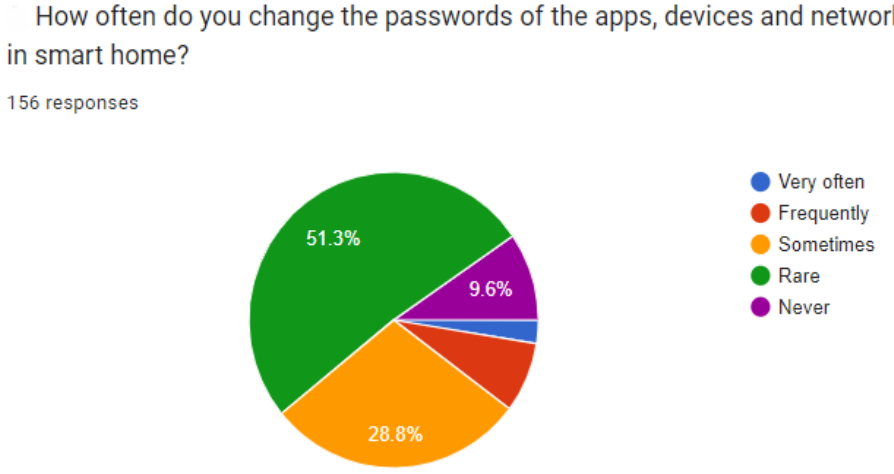

Figure 5: Changing passwords

A very large percentage of responses regarding sharing passwords with friends or neighbors or other people were negative, but it can be seen in Figure 6 that approximately 15% share their passwords.

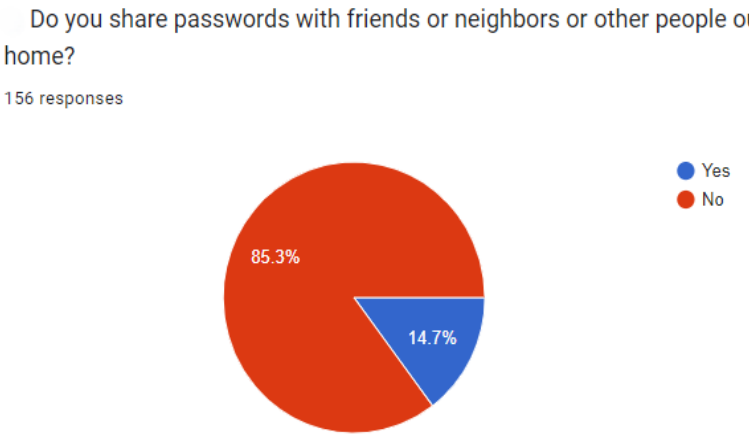

Figure 6: Sharing passwords

When asked about unique passwords used for each device or application, more than half answered negatively, which shows that the same password is used on multiple tools at home. As shown in Figure 7, approximately 40% of respondents use unique passwords for each device.

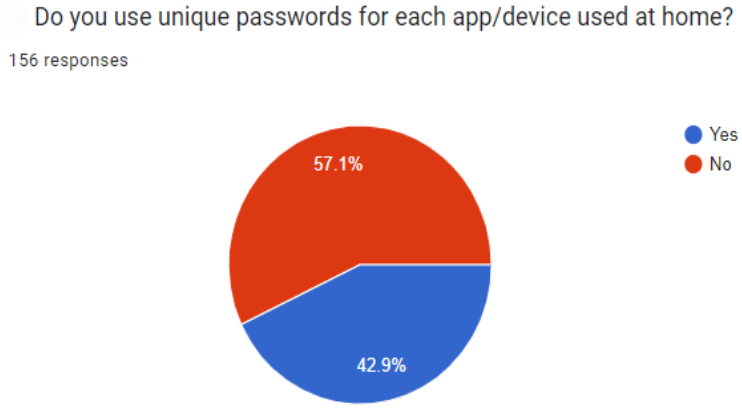

Figure 7: Unique passwords

Regarding strong passwords, Figure 8 shows that in most cases students responded that they use strong passwords. Using strong passwords makes it considerably more difficult for attacks on applications and smart devices to obtain sensitive data.

Using keywords in the password or repetitive or common structures increases the chance of identification, and from the moment a password is accessed, the path to gaining unauthorized access to the entire network is shortened.

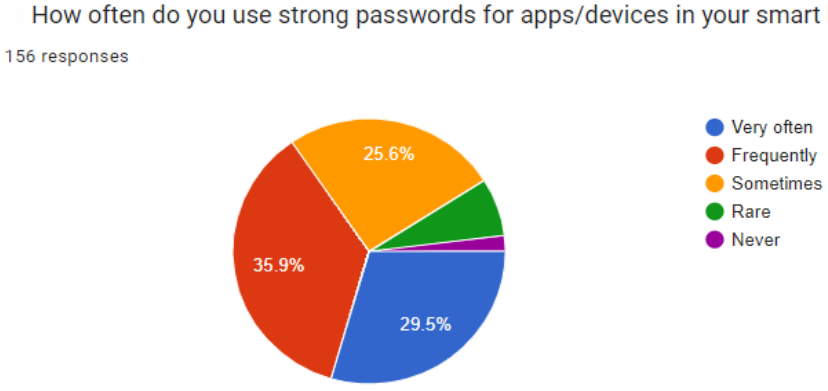

Figure 8: Strong passwords

In Figure 9, when asked about reusing old passwords, almost three-quarters answered affirmatively, which can increase the level of vulnerability on the smart products used.

There are also scenarios in which old passwords are used when changing or creating passwords that differ from the older version by one or more characters. This action is not very different from reusing old passwords in their entirety as a possibility of attack on it.

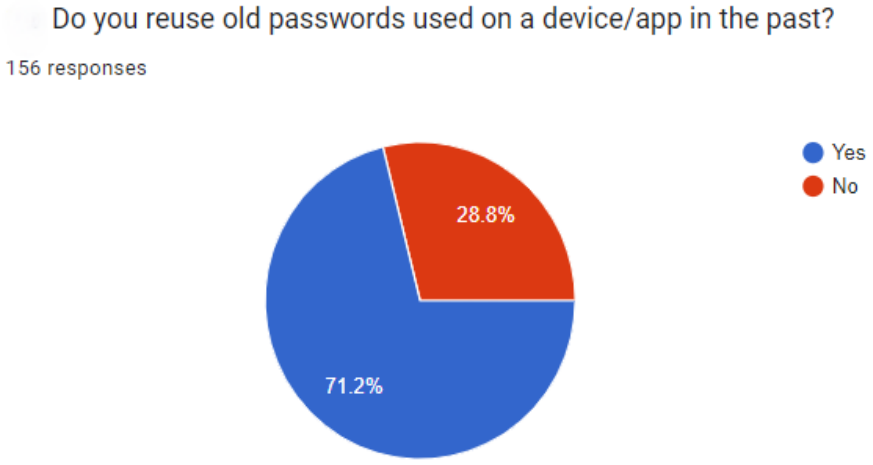

Figure 9: Old passwords

The WI-FI network is an important aspect in managing all connections in the smart home as it can influence the security of the processes that take place in real time, and WPA3 encryption brings an extra layer of security because it makes it more difficult to reach networks that use this protocol. In figure 10 it is observed that approximately two thirds of the respondents use the WI-FI network with a complex password and the WPA3 protocol.

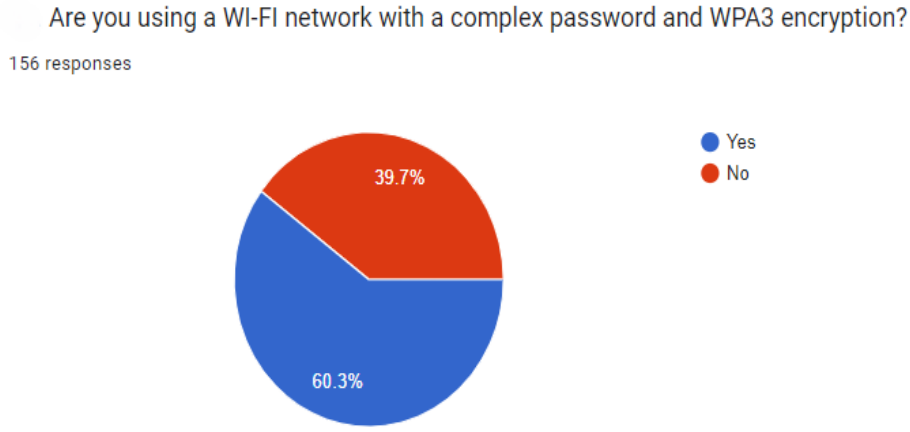

Figure 10: WI-FI network

The security settings available on devices and applications used in a smart home can be disabled by default, and the process of activating them can increase the level of security across the entire network. By using two factor authentication (2FA), even if an additional process is created at the time of authentication, the chances of possible attacks on the smart products used are significantly reduced. In figure 11, it is observed that approximately three quarters of the responses were positive, which shows that most networks use the security settings provided by the devices.

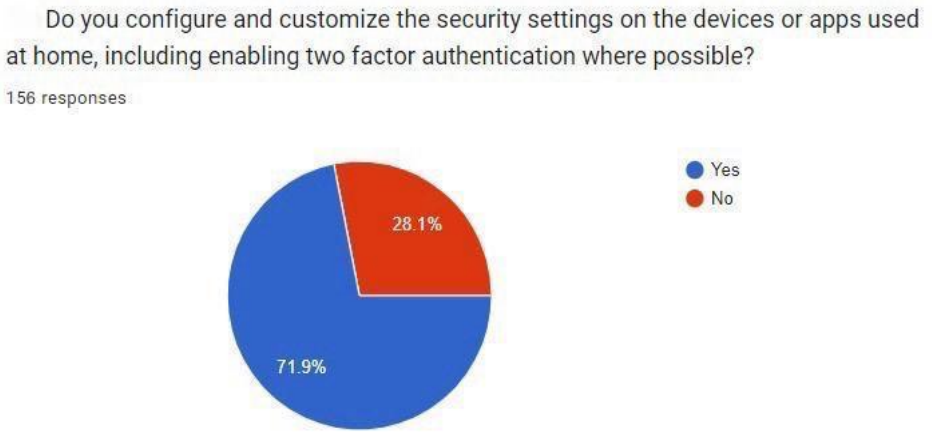

Figure 11: Security settings customization

Applications communicate with each each other inside an IoT network, but also with the outside, and this whole process is done through communication channels. In figure 12, more than half do not use secure communication channels.

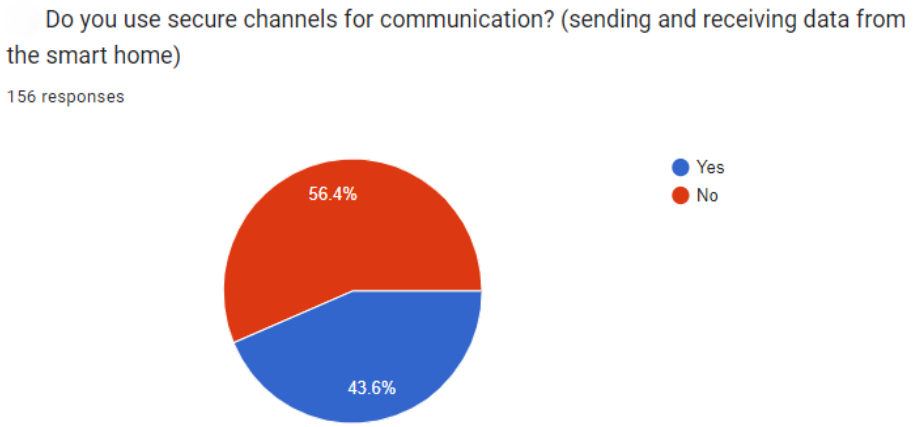

Figure 12: Secure channels

When asked about the latest existing security threats related to the smart products used, Figure 13 shows that just over 60% of respondents are not aware of these existing problems.

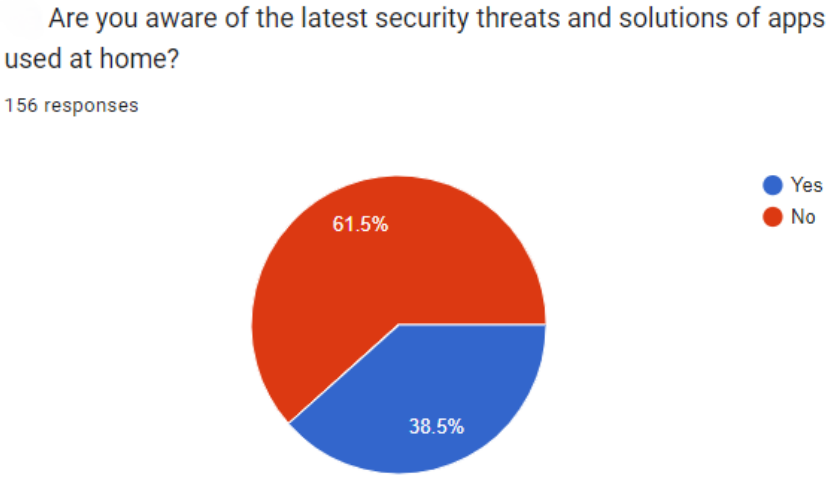

Figure 13: Latest security threats

In Figure 14, an overwhelming percentage of respondents said that all smart devices are connected to a single network. If access to the network is gained, the entire activity for all smart products can be threatened. If multiple specialized networks are used for specific processes, the risks of attacks can be significantly reduced.

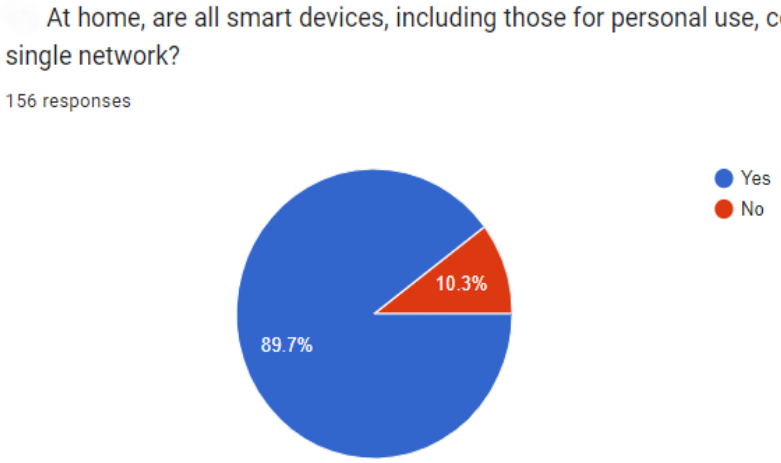

Figure 14: Single network usage

Buying smart products or using applications from reputable brands that offer security updates and technical support can help with various issues, giving a higher degree of security as the products in question have been used by many people and have proven their trust. In figure 15, approximately 80% of respondents answered affirmatively, which shows consumer trust in reputable brands.

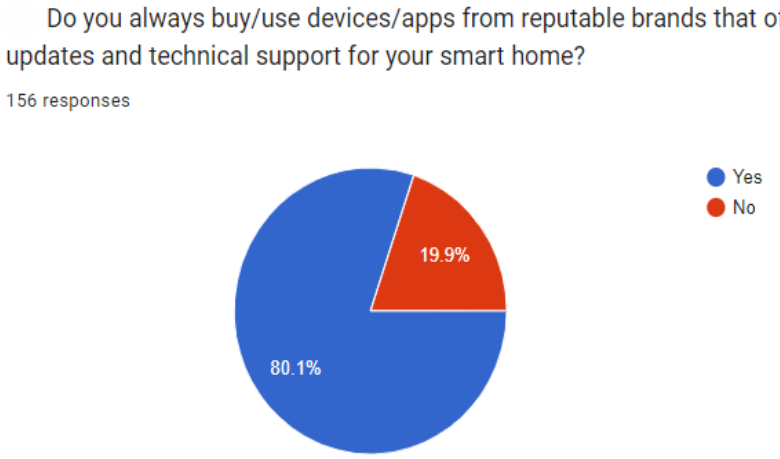

Figure 15: Reputable brands for devices and applications

Figure 16 shows that a very high percentage of respondents update to newer versions of used applications or operating systems in the case of smart devices. Periodic updates solve certain problems, including security issues, reported in older versions.

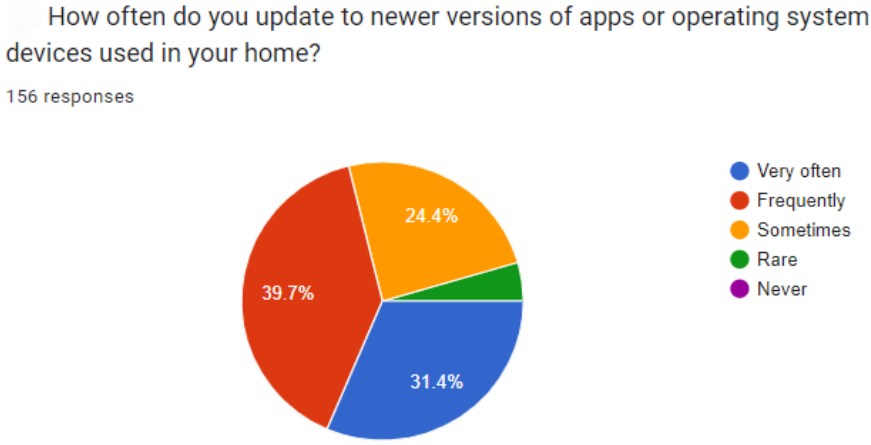

Figure 16: Updating to newer versions

4. Discussion

The actions of the residents influence the security of the smart home because through all the devices and applications used, various activities are carried out to increase the quality of life. There are several possibilities through which access to the entire IoT network can be given both involuntarily and voluntarily.

In the age of technology, there are many smart devices and applications used in smart homes, and through your phone or computer, you can even manage your home de-vices remotely. Device security largely constitutes the security of the entire network.

There are many possibilities for documenting vulnerabilities that may appear or already exist in certain versions of applications or devices. A very well-known one is Common Vulnerabilities and Exposures, a database that provides a series of information on existing problems depending on the vendors and products used. The frequency of querying and checking the devices used increases their level of security.

Knowing the functionalities of the devices and their proper use helps users both in simplifying daily processes and in improving and increasing the security of the smart home. Most respondents know the functions provided, which show that even the security part can be covered by their optimal use.

Regarding the question related to terms and conditions, the answers were divided in the sphere of less attention when installing the smart applications or services used. Through this step of reading before installation, possible problems that may be encountered during use can be identified.

Passwords are a very important point when it comes to a secure IoT network because one way to access it is by using them. There are several characteristics of passwords that must be strictly respected.

The first characteristic is that they should be changed periodically to avoid or repair processes that can be affected by different types of attacks or even by malicious intent from known individuals.

Sharing passwords both at the application or device level and at the WI-FI network level can be another problem because it gives access to sensitive data relying on the other person's correctness.

There are different scenarios when passwords are reused both in their entirety and by replacing or adding a small number of characters. This approach increases the probability of obtaining new passwords from other people.

The most recommended thing is to use strong passwords both when creating them and when changing them, this increases the security level of the smart products used since it is quite difficult to obtain or brute force attacks.

Problems can also arise at the level of the entire smart network if there are no complex passwords or more advanced standards, such as WPA3 encryption, are not used to protect existing IoT systems.

Security configurations must be set appropriately and there must be any kind of layer that significantly reduces the possibility of obtaining unwanted access from other passwords. It brings an extra step of complexity, as happens in the case of 2FA, but it makes the process of obtaining sensitive data more difficult.

Sending and priming data from the smart home must be done through secure communication channels, to protect the transmitted data since some of it may be personal.

The latest security threats can have an impact on automated processes or those managed directly by residents, and their acceptance or not can influence daily activity.

Dividing devices and applications into multiple networks that communicate with each other reduces the risk of gaining access through a single network to all the components that make it up.

Reputable brands are the most recommended when it comes to purchasing and using smart devices because they have been active for a long time, with reviews from consumers, creating a good opinion in the market.

Finally, periodic updates to newer versions of the products and services used can avoid problems that were fixed without any effort on the part of smart home residents.

From the survey conducted, there are some actions that can influence the security of smart homes, such as the management of the IoT network, the smart components that make it up, the management of passwords and how they are used, the evaluation and management of possible vulnerabilities existing on older versions that are still in use.

The 156 respondents, people specialized in the field of technology, show that there can be different ways, even involuntary ones, that can lead to obtaining sensitive data.

Building a behavior that ensures the security of smart homes by residents is becoming a necessity day by day so as not to have an impact on the quality of life and daily activities.

References

[1] Marikyan, D., Papagiannidis, S., Alamanos, E. A systematic review of the smart home literature: A user perspective. Techno-logical Forecasting and Social Change. 2019, 138, 139-154.

[2] Mouha, R. A. R. A. Internet of things (IoT). Journal of Data Analysis and Information Processing. 2021, 9(02), 77.

[3] Lin, J., Adams, B., Hassan, A. E. On the coordination of vulnerability fixes: An empirical study of practices from 13 CVE numbering authorities. Empirical Software Engineering. 2023, 28(6), 151.

[4] Zhang, H. Secure and Practical Splitting of IoT Device Functionalities (Doctoral dissertation, Carnegie Mellon University). 2023.

[5] Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., Gill, P. Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. In The 25th Annual Network and Distributed System Security Symposium (NDSS 2018). 2018.

[6] Shafiq, M., Gu, Z., Cheikhrouhou, O., Alhakami, W., Hamam, H. The Rise of “Internet of Things”: Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks. Wireless Communications and Mobile Computing. 2022, 2022(1), 8669348.

[7] Thomas, K., Pullman, J., Yeo, K., Raghunathan, A., Kelley, P. G., Invernizzi, L., Bursztein, E. Protecting accounts from credential stuffing with password breach alerting. 28th USENIX Security Symposium (USENIX Security 19). 2019. (pp. 1556-1571).

[8] Bošnjak, L., Brumen, B. Rejecting the death of passwords: Advice for the future. Computer Science and Information Systems. 2019, 16(1), 313-332.

[9] Pearman, S., Zhang, S. A., Bauer, L., Christin, N., Cranor, L. F. Why people (don't) use password managers effectively. Fifteenth symposium on usable privacy and security (SOUPS 2019). 2019. (pp. 319-338).

[10] Stobert, E., Biddle, R. The password life cycle. ACM Transactions on Privacy and Security (TOPS). 2018, 21(3), 1-32.

[11] Hall, R. C., Hoppa, M. A., Hu, Y. H. An empirical study of password policy compliance. Journal of The Colloquium for Information Systems Security Education. 2023. 10(1), pp. 8-8.

[12] Bošnjak, L., Sreš, J., Brumen, B. Brute-force and dictionary attack on hashed real-world passwords. 2018 41st international convention on information and communication technology, electronics and microelectronics (mipro). 2018. (pp. 1161-1166). IEEE.

[13] Golla, M., Wei, M., Hainline, J., Filipe, L., Dürmuth, M., Redmiles, E., Ur, B. " What was that site doing with my Facebook password?" Designing Password-Reuse Notifications. Proceedings of the 2018 acmsigsac conference on computer and communications security. 2018. (pp. 1549-1566).

[14] Halbouni, A., Ong, L. Y., Leow, M. C. Wireless security protocols wpa3: A systematic literature review. IEEE Access, 11. 2023, 112438-112450.

[15] Reynolds, J., Samarin, N., Barnes, J., Judd, T., Mason, J., Bailey, M., Egelman, S. Empirical measurement of systemic {2FA} usability. 29th USENIX Security Symposium (USENIX Security 20). 2020. (pp. 127-143).

[16] Mishra, D., Vijayakumar, P., Sureshkumar, V., Amin, R., Islam, S. H., Gope, P. Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. Multimedia Tools and Applications. 2018, 77, 18295-18325.

[17] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., Akin, E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023, 12(6), 1333.

[18] Janani, R. P., Renuka, K., & Aruna, A. IoT in smart cities: A contemporary survey. Global Transitions Proceedings. 2021, 2(2), 187-193.
[19] Herciu, M. Market capitalization, enterprise value and brand value of the world's most reputable companies. Economic and social development: Book of proceedings. 2018, 420-428.
[20] Shuhaiber, A., Mashal, I. Understanding users' acceptance of smart homes. Technology in society. 2019, 58, 101110.

Author Profile

Nicolae-Gabriel Vasilescu graduated from the Faculty of Cybernetics, Statistics and Economic Informatics in 2019. In 2021 he graduated from the IT&C Security Master program at the Bucharest University of Economic Studies and starting from 2021 he is a PhD student in Doctoral School of Economic Informatics at the Bucharest University of Economic Studies. Currently he works as Java Developer at Cegeka Romania, Bucharest. He is interested in Java programming, new technologies and IoT security.