Asian Journal of Social Science and Management Technology
ISSN : 2313-7410
Volume 6, Issue 2, March-April, 2024
Available at www.ajssmt.com

The Inhabitant as an IoT Security Factor in a Smart Home

VASILESCU, Nicolae-Gabriel Ph. D[1]

[1]*The Bucharest University of Economic Studies, Romania*

ABSTRACT : The paper presents the importance of the residents in a smart home, the decisions and behavior they have in relation to smart devices inside or outside the IoT network. Ensuring the security of the home is given by several factors, including the people who manage and make decisions about what happens in the home. There are sensitive data, such as passwords, data about people, emails, wireless, sensors that in a secure system, but through a wrong management, can be exposed to different types of attacks from the outside. Even if technology is currently evolving at a fast pace, it is important that the inhabitants are also responsible and properly use all the tools they own so that there are no leaks of information, even more so in terms of privacy. People who live and coexist in a smart home influence the security of the home in a voluntary or involuntary way by using the existing smart devices properly or not.

Keywords: - inhabitant**,** IoT, privacy, security, smart home

---

1. INTRODUCTION

Regarding smart homes, the emphasis is very often on the network that interconnects the devices inside or outside, on the security of the system, but it is rarely discussed whether the residents of the smart home influence security and privacy and if so, how this process is carried out.

Everything starts from the management of the system, how the devices are used, if they are used properly, how aware the residents are of the possible attacks that can be made on the network, from weak passwords and the level of security to the access date of inappropriate people that can very easily manipulate the network and devices in the smart home.

Another important aspect is that of ensuring network updates and operating system versions, updates that come to solve some security breaches, all these processes must take place periodically as there are multiple tools that deal with checking the systems in the interior of the smart home.

The physical security of the home must also be considered in order not to allow access at any time and under any circumstances to foreign people who do not always come authorized or only for the purpose of visits, inspections. This physical security can be managed through smart locks, appropriate alarm systems for various dangers that can happen every day.

All these behaviors encompass the security of the smart home from the point of view of the residents and their behaviors in terms of managing the activities that take place daily.

2. LITERATURE REVIEW

According to [1], IoT, short for Internet of Things, is a term used since 1999 to define a network that interconnects several smart devices and ensures communication between them, sending and receiving information from one component to another. The definition is changing in an alert way because in recent years the concept of IoT has expanded a lot as the demand for smart devices is growing rapidly.

Starting from what is reported in [2], a smart home is a home that includes several advanced technologies that facilitate the daily activities of the inhabitants, monitor, manage and control what happens in the home, devices interconnected to the IoT network main. Regarding smart homes, it is important to know the current state of both the smart devices and how the entire network is used by the residents.

In [3] it is shown that more and more people try to solve different processes at home, such as medical processes for example, and through the smart devices on the existing market, residents prefer to monitor their health directly from home. These sensitive and private data are very important for individual privacy and the security of all data is essential in a smart home.

Security in smart homes and protecting the privacy of the inhabitants is a problem that can arise and as can be found in [4], there is a set of problems depending on the new discoveries in the field, known attack types and others researched and evaluated so that residents to know in advance the possibility of these serious problems that can intervene in various activities that take place.

People's privacy is another problem that can arise at the level of the IoT network, because by stealing sensitive data it is possible to identify some passwords, some security gaps and it is possible to end up being manipulated by attackers. In [5] it shows the importance of privacy in the lives of residents and how it influences the quality of life in smart homes.

Residents influence the degree of security of the IoT system through their activities, decisions, and the use of smart devices, but as can be seen in [6], if the system is used properly, it brings performance and increases the level of user satisfaction in terms of quality of life.

In a well-designed network, certain decisions or leaks of information allow attackers to gain access to the home that they can control remotely, looking for other sensitive information to build a destructive framework on the image or decisions of the respective residents. It can happen that having certain data from a person's home, one gains access to data about another of his homes, as shown in [7], and in this case the security of many smart homes must be considered.

Each inhabitant is used to having a certain behavior and that is why images can be formed or a model can be built with each inhabitant depending on how they use the smart devices inside the IoT network, or more than that to achieve access to each application or device with the credentials of each member so that any decision or process executed has a link and the respective username to know exactly who undertakes the respective actions as in [8] this access is done using RFID.

The risks for residents are quite high, thus reaching financial or emotional losses when unauthorized persons gain access to applications or even to the IoT network, this aspect is highlighted in [9], starting from the assessment of the risks to which people are exposed who live in that house.

In [10] it is shown that residents should access the IoT network in a secure way, and in this way different problems or security breaches can be avoided. Also, any other person who should not have access to the network, is not recommended to connect and obtain access without the consent of the residents, as it appears from [11].

It is observed in [12] that communication is another important aspect in a smart home to be aware of everything that is happening and of the different activities at the security level, for example changing passwords. By the fact that every inhabitant who uses smart devices and existing applications knows the possible changes that can take place, there is a uniformity of knowledge so that no differences are created regarding the state of some components that can be perceived differently by everyone.

Also, in [13] it is shown that the residents must do certain training to correctly use the new applications or devices brought into the smart home. The proper use of all tools ensures that the chances of losing essential data decrease.

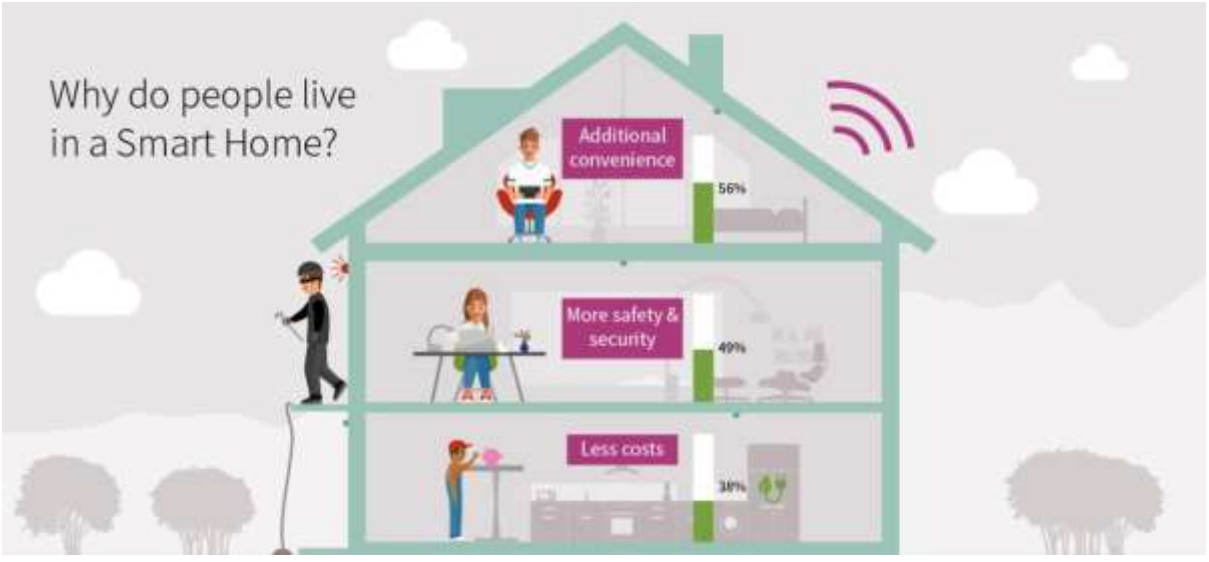
The connection between the residents must be made even when not everyone is at the smart home, as the authors show in [14], because the leakage of sensitive information can also be done remotely. There are many scenarios in which the process of remote use of some devices that manipulate certain devices in the home can be intercepted by known types of attack.

In the end, it is about the lives of the inhabitants if there is any danger, and starting from [15], the sensors that protect human life from fires, floods, gas leaks or other serious problems that can appear at any time due to different factors are vital in such moments. Residents are the main security factor in a smart home because it is primarily their life that can be affected at the level of quality of life, and more seriously, at the level of their physical health.

3. RESEARCH METODOLOGY

Residents of a smart home, in addition to the comfort they want in a smart home, are needed to correctly use the devices and applications inside that include the entire IoT system, without leaking information and without allowing access to that system by unauthorized persons.
Through all the activities that take place in the home or outside it, they gain benefits on the quality of life, through intelligent robots, devices that help with household activities, in the process of monitoring the general state of the home, heat, temperature, assisted activities from the phone or PC.
The security of the entire IoT network also brings an advantage by making a "strong smart home", and which the residents must ensure is achieved without leaving security gaps.
Obviously, costs become lower in terms of physical work, this is replaced by the automation of processes that were previously performed manually.
In Fig. 1 can be seen in miniature the processes that take place in a smart home, and the residents are in the center of attention through their daily activities, the processes they undertake, observing the advantages of the interconnectivity of devices and applications in a secure IoT network.

Figure 1. Inhabitants in the smart home



Source: Deloitte, 2018

The daily activity of the inhabitants and the automatic processes created to solve certain requirements and to replace manual tasks that were solved in the past with physical efforts must be carried out in a way that is as secure as possible from the point of view of the IoT network, as well as from the point of view of the appropriate use of smart devices. From the moment the network is secured and checked periodically, it is up to the residents to properly manage the existing security by using complex passwords to avoid their discovery by other people

or even by attackers, by not accepting all permissions from applications except for the basic ones, by denying access to the location or to the own network unless this is mandatory.

Regarding the existing sensors in the smart home, they must be tested and checked periodically because they can raise the alarm in the event of the production of some dangers that can bring health problems. Residents, in addition to increasing their standard of living and quality of life, are responsible by using technology and devices to protect their physical health from dangers, but also to carry out all their household activities in a secure manner.

Often the attacks start from the information provided by one of the residents, and from there all the information that should normally be protected starts. The focus is on confidential data, which must be separated from general data that does not have a certain impact on the security of the network or on the passwords through which access is obtained.

The updates to the latest verified versions of the devices and applications used lead to the solution of some possible security breaches, and the residents must assume that these updates take place periodically because technology evolves rapidly and thus performance and security changes take place on tools in IoT-based networks.

Communication between the residents even when they are at a distance is necessary because certain changes can occur on the network that can bring unauthorized remote access to the smart home that can become the target of possible attacks. Both the use inside the home and the use and manipulation of smart devices and applications from a distance can create leaks of sensitive information, passwords, confidential data.

The wireless network has an important role in terms of the IoT system because through it the use and influence of the entire house is reached through commands that can be brought. The lack of complex passwords and the use of personal data as passwords leads to their discovery through brute force techniques, and then even to their replacement with others, resulting in residents losing access to some technological tools in their home.

In general, the owners of the house have full access to the IoT system and further propagate the authorized access to the other residents according to each one's needs. In this way, unauthorized access is also avoided from inside the home, for example, children have limited access to the devices and applications used in the home so that various unwanted actions do not happen.

Security at the physical level of the smart home is an important aspect because a network based on IoT with a high level of security but in which it is possible to enter and leave easily at the physical level attracts possible infiltrations by malicious people who can cause thefts or break-ins of smart devices.

To combine the secure system with the proper use of the IoT network by the inhabitants of a smart home, it is necessary to periodically check the home, the devices and applications used, as well as for people to learn how to use and manage the automation of household activities.

The inhabitant, as the main factor in the security of the smart home, is the one who helps to keep the data safe and ensures that he takes all the necessary actions in order not to disclose sensitive information to the outside that can later be used against him in different ways.

4. FUTURE WORK

Soon my proposal to carry out a survey to identify to what extent the residents of smart homes are prepared from the point of view of IoT security to use smart devices and applications without creating leaks of sensitive information and without allowing unauthorized access to their own housing.

The existence and use of tools to show whether a smart home is vulnerable or not to possible known and already researched attacks is another aspect of interest, and their implementation as a necessity shows the degree of security of the home and the possible updates on systems that solve security problems being quite useful.

There is a need for checks on the smart home in terms of possible security breaches that may appear, considering that technology evolves at a fast pace, and the residents of the smart home are responsible for the level of security through the activities and processes they perform.

The challenges regarding the evolution of technology are also a subject of interest because from month-to-month features appear that solve certain problems that occurred in the past and that could bring losses in terms of the person or even the home.

5. CONCLUSIONS

The residents of a smart home are the main security factor because they are involved in the activities that take place daily and in the automated processes that improve their lives, but besides these aspects, their physical health can be affected if certain events or dangers occur. inside or outside the house.

They can influence the IoT network by giving access to people who are ill-intentioned or by leaking information that can be done involuntarily, but for this reason there could be different attacks on the entire system.

Training regarding new applications brought into the smart home or devices that have not been used before is recommended to increase security and to properly use the functionalities brought to increase the quality of life.

Updates to newer versions can avoid the occurrence of certain attacks because they solve issues that were discovered in the past and that caused damage even on a financial level. These periodic updates ensure a high level of security and the possibility of avoiding problems that can even lead to the loss of certain sensitive data.

Residents can use different tools to test different security breaches and to fix the problems, thus generating a fix for the various technological leaks.

The atmosphere and the quality of life, through the automation of processes, the use of intelligent robots, is given by the inhabitants, by every action taken at the level of technology that can sometimes cause a low degree of security through various actions or activities performed in a way that is not optimal.

6. REFERENCES

[1] D. R. Berte, Defining the iot, *Proceedings of the international conference on business excellence*, 12(1), 2018, 118-128.

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

[3] K. Fouquet, G. Faraut, and J. J. Lesage, Model-based approach for anomaly detection in smart home inhabitant daily life, *2021 American Control Conference (ACC),* 2021, 3596-3601.

[4] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, Smart home security: challenges, issues, and solutions at different IoT layers, *The Journal of Supercomputing*, *77*(12), 2021, 14053-14089.

[5] N. Guhr, O. Werth, P. P. H. Blacha, and M. H. Breitner, Privacy concerns in the smart home context, *SN Applied Sciences*, *2*, 2020, 1-12.

[6] D. Mocrii, Y. Chen, and P. Musilek, IoT-based smart homes: A review of system architecture, software, communications, privacy, and security. *Internet of Things*, *1*, 2018, 81-98.

[7] E. Zeng, and F. Roesner, Understanding and improving security and privacy in {multi-user} smart homes: A design exploration and {in-home} user study, *28th USENIX Security Symposium (USENIX Security 19),* 2019, 159-176.

[8] Z. Shouran, A. Ashari, and T. Priyambodo, Internet of things (IoT) of smart home: privacy and security, *International Journal of Computer Applications*, *182*(39), 2019, 3-8.

[9] B. Ali, and A. I. Awad, Cyber and physical security vulnerability assessment for IoT-based smart homes. *sensors*, *18*(3), 2018, 817.

[10] S. Chitnis, N. Deshpande, and A. Shaligram, An investigative study for smart home security: Issues, challenges and countermeasures, *Wireless Sensor Network*, *8*(4), 2016, 61-68.

[11] J. Bugeja, A. Jacobsson, and P. Davidsson, an analysis of malicious threat agents for the smart connected home, *2017 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops)*, 2017, 557-562.

[12] F. Cicirelli, G. Fortino, A. Giordano, A. Guerrieri, G. Spezzano, and A. Vinci, On the design of smart homes: A framework for activity recognition in home environment, *Journal of medical systems*, *40*, 2016, 1-17.

[13] S. Zhang, S. McClean, B. Scotney, P. Chaurasia, and C. Nugent, using duration to learn activities of daily living in a smart home environment, *2010 4th International Conference on Pervasive Computing Technologies for Healthcare*, 2010, 1-8.

[14] P. Baudier, C. Ammi, and M. Deboeuf-Rouchon, Smart home: Highly-educated students' acceptance, *Technological Forecasting and Social Change*, *153*, 2020, 119355.

[15] J. Vanus, J. Belesova, R. Martinek, J. Nedoma, M. Fajkus, P. Bilik, and J. Zidek, Monitoring of the daily living activities in smart home care. *Human-centric Computing and Information Sciences*, *7*, 2017, 1-34.

Info

Corresponding Author: VASILESCU, Nicolae Gabriel, The Bucharest University of Economic Studies, Romania.

How to cite this article: VASILESCU, Nicolae Gabriel, The Inhabitant as an IoT Security Factor in a Smart Home. *Asian. Jour. Social. Scie. Mgmt. Tech*. 2024; 6(2): 129-134.