sciendo

Proceedings of the 5th International Conference on Economics and Social Sciences (2022), ISSN 2704-6524, pp. 917-923

The 5th International Conference on Economics and Social Sciences
Fostering recovery through metaverse business modelling
June 16-17, 2022
Bucharest University of Economic Studies, Romania

IoT Security in the Context of Digital Organizations

Nicolae-Gabriel VASILESCU[1]

DOI: 10.24789788367405072-085

Abstract

The main goal of this paper is to identify security issues related to the use of IoT devices in a private or public organization and to propose innovative solutions to solve the problems found. The paper also contains an analysis of the current context and how the part of innovation within a company can be impacted both in terms of overall image and punctuality in the process of finding new solutions by affecting or vulnerabilities that may be exposed through components in the sphere of IoT. The issue of money and how it can create huge losses due to security breaches or possible cyberattacks on the components used at the IoT level is another important aspect that appeared from the analysis performed in this paper. In the end, the analysis performed and the solutions found bring a high yield related to the innovation process within the specialized centers within the private or public companies.

Keywords: IoT, security, innovation, vulnerabilities.

JEL Classification: O36.

1. Introduction

In recent years, both in the sphere of private organizations and public institutions, there has been an ascending trend in the use of smart devices or technology based on the Internet of Things regarding the digitization process. This is due to the need to automate many processes that were previously performed manually.

The Internet of Things, abbreviated as IoT, is for many people a real infrastructure that connects millions of new smart devices that communicate with each other or on the Internet and share data, often sensitive, as explained by Berte and Clara (2018).

The current emphasis is on innovation, with many companies forming dedicated teams for this process. It creates a good image from the outside in this context, attracting new employees who want to develop and find new and smart solutions. The IoT component has an important role in all this setting, helps to significantly improve the results and facilitates the work that the user does to collect information and data that is sensitive.

[1] Bucharest University of Economic Studies, Bucharest, Romania, gabriel.vasilescu@csie.ase.ro.

In most cases, the use of Internet of Things components is encouraged, especially when it comes to modernizing the public system or innovating in private companies, but a big problem in this regard is at the level of IoT security. Various types of attacks can occur here that can produce the loss of sensitive information, huge loss of money, and destruction of the public image.

There is a need to protect these components that facilitate the daily data collection process, through various means, periodic testing by dedicated people, or their improvement by upgrading to the latest technologies in the field that certainly come high compared to previous versions.

The digitization process at the organization level helps people who use the services offered by companies or public organizations to improve their quality of life, but in addition to this, they also need the protection of personal data. In this case, the security issues that may arise from the use of applications and smart devices are a real problem, and many funds are being made available to dedicated companies to solve them.

In addition to the technology that is advancing day by day, problems can arise from within digital organizations by exposing data, and there can also be malicious people from outside who want to find out sensitive information or create a wrong image for users. The same problem arises in the case of public organizations, on which cyberattacks can occur in order to access valuable information belonging to the state.

2. Problem Statement

As shown by Velsberg et al. (2020), the digitization of the state level using the Internet of Things is done by combining technologies, people, and organizations, with more emphasis on the desire for a modern action that is first done manually on the use of appropriate technologies. Most of the time, the whole process of building smart processes in both public and private organizations is postponed, or they are not discussed as real problems and of immediate impact, they are put at the end of the list of priorities.

Digitization in education has grown in recent years due to the need to automate the learning process, make it easier using smart devices and applications based on IoT technology add value, but also make this activity more interactive and beneficial for both teachers and students, as Stroe (2021) researched.

The integration of IoT components emphasizes the dimensions of efficiency, effectiveness, transparency and collaboration. In other words, security issues may occur if one of the 4 features is not met.

At the level of the public sector, Kankanhalli et al. (2019) identified the challenges that appear in the implementation and adoption of these technologies in order to transform the state system into a high-performance one, emphasizing the degree of responsibility, fairness, and ethics within. Employees working to provide intelligent solutions in the public domain must have the three characteristics in the process of creating and building a digital and innovative environment. IoT security has no value if the elements discussed above are not checked.

Roman-Castro et al. (2018) point out that in recent years both the public and private sectors have continued to explore different paradigms and areas of application that involve connecting all these objects. Moreover, this IoT domain continues to evolve, and its security capabilities must keep up with the same trend. One of the main factors that lead to distrust of using IoT as a secure source is realizing that IoT objects can become their own adversary. This is because web hosts can in some cases be owned by malicious parties or are remotely controlled by exploiting vulnerabilities.

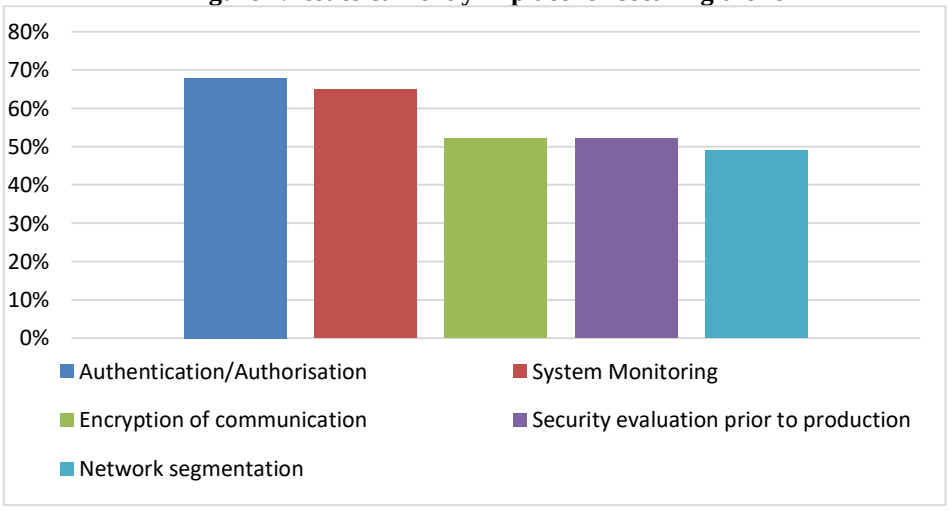
As AboBakr et al. (2017) explained, we meet different technologies inside IoT systems: sensors, 3G, 4G, NFC, RIFD used in the transfer of private data, extremely sensitive and very large in volume. Users who are using these technologies need to consider a number of issues, including the possibility of cyberattacks, ethical and legal issues that are shaping the health of IoT applications.

Miniaturization issue is another problem encountered, going to the nano size level in the case of IoT devices. The process of controlling their quality, data traffic, and security at the bottom point is becoming more difficult.

Also, the IoT globalization brings problems because sensitive data is transmitted from the countries where smart devices are used in the country that offers those services, the medical services are an example.

Tankard (2015) has shown that the main security issues regarding IoT applications are: allowing the use of weak passwords, access to some sensitive information from the huge amount that is transmitted from and to the applications used, the data sent is not encrypted, cross-issues site scripting at the level of web interfaces, and software updates that are not encrypted when downloaded. The solution of the security challenges consists of treating in a special way the following 5 processes according to Figure 1.

Figure 1. Issues currently in place for securing the IoT



Source: SANS Institute.

These problems in the context of digitization are common and harm to users because the confidentiality of their own data is not ensured.

As can be seen in the paper written by Oser et al. (2020), another IoT security approach is to make users to be aware of the risks and problems that arise when using these smart devices. Users should know what risks they face if they do not follow a certain requirement, such as the current standard for setting passwords at the application level.

Sestino et al. (2020) explain that digitization eases the connection between technology and management for users, but there are still some question marks about the potential of the IoT domain, which has created a disorganized high level of knowledge.

The opportunities and challenges that arise when integrating IoT into the digitalization of companies or public organizations are closely related to the security side and the trust or understanding of smart applications.

3. Aims of the Research

The analysis is based on the identification of security issues at the IoT level in the context of the digitization of private and public organizations. Infrastructure problems can occur, such as how applications are connected to sensors, internet access in a certain area, weather conditions, and other important issues. Also, at the level of applications or smart devices we find many security breaches, which allow different types of attacks to access sensitive information inside. The user's awareness of the components of IoT security contributes to the avoidance of problems that may arise; an example is the need to use strong passwords to avoid breaking them. If the application user is aware of what to use and how to use it properly, many of the attacks and problems can be attenuated.

The current vulnerabilities in the IoT area are another point of interest as it helps to create real solutions in applications that help to digitize public organizations or the private environment.

Another important aspect is how the end user or the citizen can be helped in the case of public organizations in order to avoid the security problems that may occur without him realizing them. What are the ways in which he learns to properly use digital applications and devices that optimize his effort in solving certain tasks, payments, signing documents, or other operations in that case?

Given the security issues identified, users need an application to check how vulnerable an IoT-based application is to the current issues in this area and to make them aware that the use of IoT components involves a risk when they do not know the real problems and how their data may reach into a public image or in possession of malicious people.

4. Research Methods

Starting from the current situation regarding the security of IoT applications and devices in the context of digitalization of private and public organizations,

an essential aspect is that of teaching users about security breaches that can lead to finding their own sensitive information, control, and the identification by another person of the actions performed by the citizen or by a simple user.

It is important that the user does not offer himself the possibility of an attack on his own data, to have strong passwords, to ensure that the documents are signed and saved securely, and all processes are safe and in accordance with the law.

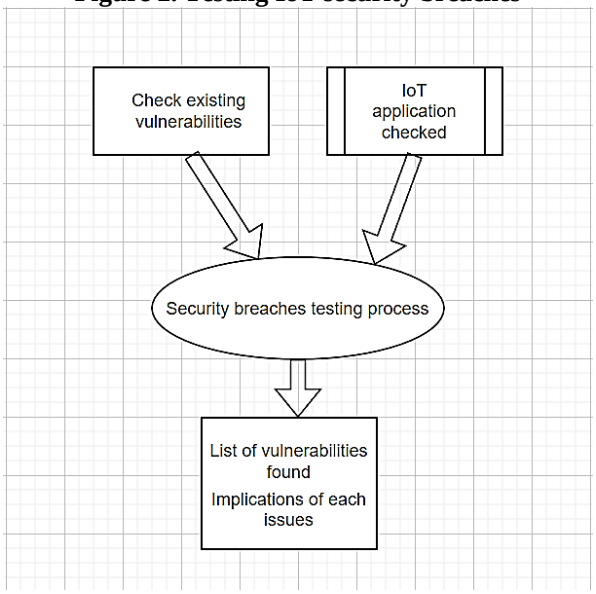
Because this need to know about security issues in smart apps was identified, a prototype app is needed to help users and inform them of vulnerabilities in state-owned or private IoT-based applications they use.

From the collection of vulnerabilities found by Rytel et al. (2020) and currently available for smart devices and applications, a division will be made according to the degree of risk to which a user may be exposed, the problems with major risk will be signaled in the application with red color. In their case, it is chosen not to use that IoT-based application provided by the public or the private digital organization until it is fixed, with the necessary explanations regarding the losses that may occur.

There will be problems with medium risk, and in this case they will be indicated with yellow color. In this case, depending on the severity of the situation, it is possible to choose or not to use the application. The positive scenario is one in which no issues are detected, and this is marked with green.

This model aims to identify new vulnerabilities in IoT-based applications or devices every time and to check if the applications needed by users are experiencing these problems or not. Each time these vulnerabilities will be updated, and from each application test, the user will know if he encountered by those problems as shown in Figure 2.

Figure 2. Testing IoT security breaches



Source: Own figure.

In addition, all identified security breaches will have explanations so that it is known exactly what the implications of using an application are.

Another advantage is that information can be addressed to the relevant digital organizations or state institutions either to upgrade the IoT components used to the final versions or to fix the identified security issues.

As Pocatilu et al. (2020) shows, CVSS (Common Vulnerability Score System) is a standard found in companies to identify vulnerabilities in IoT-based devices and applications. This score helps users to know the security level of smart applications used, and at the time of their use, there are no problems related to the stealing of personal data.

5. Findings

The expected results are based on two directions, the first one is related to the public or private applications based on IoT technology that are checking if the vulnerabilities currently exist or have not upgraded to the latest version that solves the detected problem, and the second one is based on users' understanding and awareness of the current problems and how they can suffer data loss, which ultimately leads to huge loss of money and destruction of personal image.

It is quite useful for users of smart applications, as a result of digitization, to have data in safe and the safe use of various resources exposed by private or public organizations, without data loss or control of other entities on the steps taken.

Taking into account the CVSS, the user will know the security level of the smart application he is using and whether he can use it or not, receiving recommendations that will make him make the right decision.

6. Conclusions

Given the need to protect the data of citizens or users of applications based on IoT technology in the digital age, an application is needed to check the current vulnerabilities in the applications provided and also to expose the consequences that may occur and how can the cyberattacks exist due to unresolved issues.

With the expansion of all IoT-based applications and smart devices in the current digitalization situation, a lot of security problems arise, with users being exposed both cyberattacks and personal data exposure without realizing it.

Depending on the severity of the problems identified, the user may decide to continue using IoT-based applications until the issues are resolved. In the context of digitization, we must be careful to protect data, to prevent, and combat security problems that may occur in the life cycle of an application or a device.

The need to build an application based on the prototype described above was noticed to help users to identify vulnerabilities, making them aware of existing security issues in terms of IoT-based devices and applications. People who use these components should also see what issues are being addressed by certain upgrades.

Acknowledgment

This paper was co-financed by The Bucharest University of Economic Studies during the PhD program.

References

[1] AboBakr, A., Azer, M.A. (2017). IoT ethics challenges and legal issues, *12th International Conference on Computer Engineering and Systems*, pp. 233-237.

[2] Berte, B.R., Clara, S. (2018). Defining the IoT, De Gruyter, pp. 118-129.

[3] Kankanhalli, A., Charalabidis, Y., Mellouli, S. (2019). IoT and AI for Smart Government: A Research Agenda, *Government Information Quarterly*, 36(2), pp. 304-309.

[4] Oser, P., Feger, S., Wozniak, P.W., Karolus, J., Spagnuelo, D., Gupta, A., Luders, S., Schmidt, A., Kargl, F. (2020). SAFER: Development and Evaluation of an IoT Device Risk, *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 4(3).

[5] Pocatilu, P., Zamfiroiu, A., Apostol, V. (2020). Automated Analysis of Topics on Security, *Informatics and Control*, pp. 459-469.

[6] Rytel, M.F., Felkner, A., Janiszewski, M. (2020). Towards a Safer Internet of Things A Survey of IoT, *Sensors*, pp. 1-26.

[7] Roman-Castro, R., Lopez, J., Gritzalis, S. (2018). Evolution and Trends in IoT Security, *Computer*, 51(7), pp. 16-25.

[8] Sestino, A., Prete, M.I., Piper, L., Guido, G. (2020). Internet of Things and Big Data as enablers for business digitalization strategies, *Technovation*, 98.

[9] Stroe, A.C. (2021). Teachers' Perspective on Integration of Mobile Solutions in Romanian, *Informatica Economică*, pp. 75-88.

[10] Tankard, C. (2015). The security issues of the Internet of Things, *Computer Fraud & Security*, 2015(9), pp. 11-14.

[11] Velsberg, O., Westergren, U.H., Jonsson, K. (2020). Exploring smartness in public sector innovation - creating smart public services with the Internet of Things, *European Journal of Information Systems*, 29(4), pp. 350-368.