Research, Society and Development, v. 10, n. 2, e57010212917, 2021
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v10i2.12917

# Criticality assessment of the components of IoT system in health using the AHP method

## Avaliação de criticidade dos componentes de um sistema IoT na saúde usando método AHP

## Evaluación de la criticidad de los componentes de un sistema IoT en salud, utilizando el método AHP

Received: 02/12/2021 | Reviewed: 02/18/2021 | Accept: 02/22/2021 | Published: 02/28/2021

**Erika Midori Kinjo**
ORCID: https://orcid.org/0000-0002-6348-6162
Universidade Nove de Julho, Brasil
E-mail: midori.kinjo@gmail.com
**André Felipe Henriques Librantz**
ORCID: https://orcid.org/0000-0001-8599-9009
Universidade Nove de Julho, Brasil
E-mail: librantzandre@gmail.com
**Edson Melo de Souza**
ORCID: https://orcid.org/0000-0002-5891-4767
Universidade Nove de Julho, Brasil
E-mail: prof.edson.melo@gmail.com
**Marcelo Galdino**
ORCID: https://orcid.org/0000-0002-4227-964X
Universidade Nove de Julho, Brasil
E-mail: lgmgaldino@gmail.com

**Abstract**
The Internet of Things (IoT) network in the health area offers many facilities or conveniences, as it allows communication between machines, such as monitoring the development of chronic diseases, disseminating disease control, monitoring the fall of the elderly. However, this communication can bring some associated risks, such as breach of privacy and security, loss of data integrity. Thus, this study identified the components of the network that interfere with the occurrence of risk and their respective hierarchy within the IoT system used in the health area. There were 8 (eight) factors identified in the literature and were validated by 2 (two) academic experts with knowledge on the subject. The use of the Analytic Hierarchy Process (AHP) method allowed to identify the most critical componentes related to the study proposed here.
**Keywords:** Internet of things, IoT; Analytic hierarchy process; Risk; Health.

**Resumo**
A Internet das Coisas (IoT) na área da saúde oferece muitas facilidades ou conveniências, pois permite a comunicação entre máquinas, como acompanhar o desenvolvimento de doenças crônicas, disseminar o controle de doenças, monitorar a queda de idosos. No entanto, essa comunicação pode trazer alguns riscos associados, como violação de privacidade e segurança, perda de integridade dos dados. Assim, neste contexto, este estudo identificou os componentes da rede que interferem na ocorrência de risco e sua respectiva hierarquia dentro do sistema de IoT utilizado na área da saúde. Houve identificação de 8 (oito) fatores na literatura e foram validados por 2 (dois) especialistas acadêmicos com conhecimento sobre o assunto. A utilização do método Analytic Hierarchy Process (AHP) permitiu identificar os componentes mais críticos relacionados ao estudo aqui proposto.
**Palavras-chave**: Internet das coisas; IoT; Analytic hierarchy process; Risco; Saúde.

**Resumen**
El Internet de las Cosas (IoT) en el área de la salud ofrece muchas facilidades o comodidades, ya que permite la comunicación entre máquinas, como monitorear el desarrollo de enfermedades crónicas, difundir el control de enfermedades, monitorear la caída de los ancianos. Sin embargo, esta comunicación puede traer algunos riesgos asociados, como violación de la privacidad y seguridad, pérdida de la integridad de los datos. Así, en este contexto, este estudio identificó los componentes de la red que interfieren con la ocurrencia del riesgo y su respectiva jerarquía dentro del sistema IoT utilizado en el área de salud. Se identificaron 8 (ocho) factores en la literatura y fueron validados por 2 (dos) académicos expertos con conocimiento en el tema. El uso del método Analytic Hierarchy Process (AHP) permitió identificar los componentes más críticos relacionados con el estudio aquí propuesto.
**Palabras clave**: Internet de las cosas; IoT; Analytic hierarchy process; Riesgo; Salud.

## 1. Introduction

The vision of a connected world enables more intelligent, sustainable and inclusive economies, requiring resources related to ubiquity, reliability, high performance, efficiency and scalability (Biswas & Giaffreda, 2014). Likewise, the Internet of Things (IoT), a term created by Kevin Ashton in 1999 (Greengard, 2015), has evolved and gained notoriety in scientific communities and by other researchers. So, the term IoT can be defined as the ability of multiple devices to interact with each other on a network with the presence of a limited or nonexistent user (Mena, et al., 2018). The basis for controlling this interaction occurs through other objects, systems and servers (Radanlieva, et al., 2020). The WSN (Wireless Sensor Network) and the M2M (Machine to Machine Communication) can be considered as examples of IoT networks (Lee & Ouyang, 2014)

The Internet of Things has been permeating the daily lives of companies and people (Ray, 2017), being applied to monitor and track the goods lost during the logistical delivery process (Ben-Daya, et al., 2017). In agribusiness, for instance, it has been used in pest control and soil quality (Lin, et al., 2019), and control of agricultural supplies (Yan, et al., 2017). Besides, in sports it has been applied aiming at a preventive monitoring of athletes' injuries (Wilkerson, et al., 2018). The application in education is also a worldwide trend that impacts on the physical and virtual learning environment (Elsaadany & Soliman, 2017).

The health area was one of the first to adopt the IoT (Lomotey, et al., 2017) and it has been applied to improve the quality of services, providing mobility and autonomy in daily activities (Domingues, et at., 2019 ). In order to improve medical services in hospitals, wearable systems are used to detect emergency cases at the time of screening (Albahri, et al., 2019). In the context of mobility, there are works that utilize sensors to capture plantar pressure and thereby identify, during walking, posture problems in spine and diabetic foot ulcerations (Domingues, et al., 2019). Another example of its application in the health area is to control the development of chronic diseases. In order to prevent problems, Ali et al. (2018) suggested supervising patients, using sensors, after recommending diets with specific foods and medications.

Therefore, the application of the IoT in health shows promising benefits for the patient's well-being, such as remote monitoring and/or diagnosis (Albahri, et al, 2019). However, some issues may jeopardize the application of this emerging technology. For instance, changes in the data package (data inconsistency) and in the generation of incorrect data may occur during the remote monitoring process (Sharma & Chen & Sheth, 2018). Besides that, another challenge is to maintain the privacy of adverse data from the network, allowing its analysis or not, jeopardizing the benefits of its application (Sharma & Chen & Sheth, 2018).

**Related Works**

**IoT system risk**

A modern healthcare system involves a data mesh in order to continuously monitor the patient. Sensors transmit patient data (blood pressure, heart rate, oxygen saturation, temperature, among others), which are stored and analyzed. For this, privacy must be maintained at all stages of the process so that the benefits of using the network are achieved. However, this ideal privacy is practically unattainable (Sharma & Chen & Sheth , 2018; Sood & Mahajan, 2017; Wang , 2018).

In addition to studies involving risks related to privacy and security, there are studies considering risks related to data integrity (Lomotey et at., 2017); Muhammed et al, 2018), the authors suggest solutions related to the protocol, Device/Sensor and to the Gateway. When evaluating a specific context, restrictions to the proposals presented have to be taken into consideration. They can indicate that it is not possible to implement the best algorithms to model the healthcare (Sharma & Chen & Sheth , 2018) or just to give evidence only to one aspect of the network to be mitigated such as latency, bandwidth, energy consumption and other parameters (Muhammed et al., 2018).

It becomes vital for the successful implementation of these modern health systems to focus on a component of the network and distribute the workload among its participants in order to mitigate these risks involved (Sharma & Chen & Sheth,

2018). And ethic issues were pointed as an external component to the network security (Mittelstadt, 2017 [1], Mittelstadt, 2017 [2]).

**IoT system risk evaluation**

The application of techniques or methods to evaluate health risks IoT, are currently restricted to a few articles. For instance, Petri network technique has been applied in the development of a wearable IoT data flow architecture that offered traceability of data routes from the source to the health information system in order to determine what data belongs to whom efficiently. (Lomotey et al., 2017).

Gyamfi et al. (2019) proposed the Bayes method to obtain an ideal balance between minimizing the energy cost of pulse transmission and reducing the incidence of important losses during the transmission of patient data, such as heart rate. In addition, they proposed an ideal protocol for transmitting this type of data

In another application Analytical Hierarchy Process was applied to improve the screening of patients, selecting hospitals according to the patient's emergency. This enabled improvement in medical team organizations in a modern lifestyle and better supporting the needs of the patient (Albahri, et al., 2019).

Moreover, Huang et al. (2018) applied the AHP technique to evaluate risks in IoT systems, but without focus on the health area. In the mentioned studies, the analysis techniques were not used in the joint analysis of the components of the IoT network in the health area, but in a specific component. In addition, they do not assess the criticality of components external to the network.

In this context, the main contributions of this work are: (1) identification, in the literature, of the main components of the IoT network in the health area, highlighting the inclusion of external components in the analysis (2) definition of ranking of the network components utilizing the Analytic Hierarchy Process (AHP) technique. And, in the practical scope: development of a support tool for managers to assess the criticality of each component in the IoT network in the health area.

This article is structured in 4 sections. The first section presents the methodology utilized. Afterwards, it is presented the theoretical basis and discussion of the results. And then, it is concluded with the considerations of the study, presenting limitations and suggestions for future studies.

## 2. Methodology

The study adopted mixed approach, as it combined strong points of the qualitative and quantitative approaches (Creswell, 2010). Conforming Pereira et al (2018), the qualitative approach was chosen to assign a level of relevance and also to the probability of failure of the components of the Internet of Things system and was carried out with the help of specialists. The specialists were provided with the options “Little relevant”, “Medium” and “Very Relevant” and to assign the probability of failure the options were: “Very low”, “Low”, “Median”,“ High ”,“ Very high ”.

The use of a qualitative approach to obtain this information tends to decrease the amount of adverse errors. Each of the options requires conversion to conversion to numerical values and therefore requires more care. Therefore, these numerical values were used in a quantitative approach, when using as the initial parameterization of the AHP.

In addition, according to Kumar (2011), research can still be classified as to its purpose. This research initially had an exploratory character, since the initial focus was to provide context about the studied problem. In a second step, the study became predominantly descriptive, in which there is a deepening on the theme. It is at this stage that prior knowledge obtained in the exploration of the problem situation is considered.

This work was divided into 4 (four) steps, as follows: (1) The literature review, (2) Application of the AHP method, (3) ranking determination and (4) evaluation of the consistency rate, which.

## 3. Literature Review

In the literature review, the database of Scopus, Web of Science and IEEE Explorer were consulted, utilizing the combination of key-words: IoT and Risk and Health, ′Internet of Things′ and Risk and Health, IoT and failure and health, ′Internet of Things′ and failure and health of the last 5 years. And from the results of these searches, the criteria of proposed and adapted selection (Liao, et al., 2017) resulted in 55 articles. The literature indicated eight components of the IoT network that were listed in Table 1.

The components, their respective examples and respective authors that corroborate were listed in Table 1.

**Table 1 –** IoT components, definition and example.

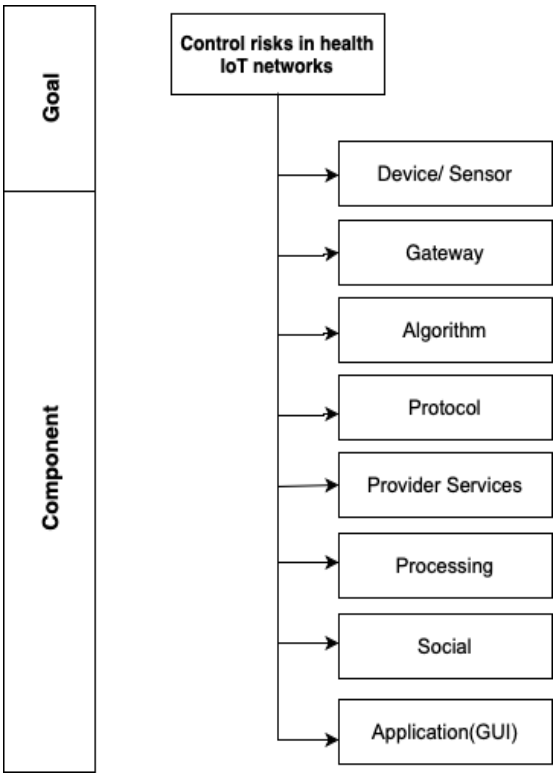
| Component | Concept | Example | studies that corroborate |
|---|---|---|---|
| Device/ Sensor | Responsible for collecting data about health related symptoms and various events inside and surrounding environment related to the user. The collected data include areas: health, environmental, medicinal, location and meteorological data. Data are collected from the wireless hardware devices embedded into the user's body, inside and surrounding places of user. | Wearable, Body Area Network, Personal Healthcare Device (PHD) | Sood & Mahajan (2017), Wang (2018), Muhammed et al. (2018) |
| Gateway | Is an interconnection and services management platform. The main role of the gateway is connect the Wireless Sensor Networks (WSNs) with public communication network, so gateway is needed to work as protocol translators, impedance matching devices and rate converters between them. | access point, Wireless Transmission (SIM7000C (NB-IoT) ) | Wang (2018), Hu et al. (2019), Azimi et al. (2019) |
| Algorithm | Acts as a bridge between IoT sensors and Provider Services. It is used for real time processing and analysis of accumulated data from IoT based sensors. | Embedded algorithm, cryptography , Genetic Algorithm, AODE algorithm | Sood & Mahajan (2017) ,Wang (2018), Albahri et al (2019) |
| Protocol | Allow interoperability across the heterogeneous networks and seamlessly allow data exchange throughout IoT system | Shamir's secret sharing, LEACH protocol (cluster), IKEv2, IPv6, oneM2M | Mittelstadt (2017), Sharma & Chen & Sheth (2018), Wang (2018), Muhammed et al. (2018) |
| Provider Services | Store patients' data (encrypted, perturbed, or anonymized, and without any Personally Identifiable Information (PIIs)), and are preocuped data mining and maintaining propriety of the collected data and learned models. May choose to outsource data and computation to a cloud provider that delivers infrastructure for storage and analytics. | Public or private cloud | Sood & Mahajan (2017), Sharma & Chen & Sheth (2018) |

| | | | |
|---|---|---|---|
| Processing | Vital activity to distribute total workload of privacy- preserving frameworks to their participants relative to the resources available. A practical framework must ensure the resource- constrained parties perform lighter complexity tasks, while the expensive tasks be parallelized at the resource-abundant party such as a cloud. | Parallel, Distributed | Sharma &Chen & Sheth (2018) |
| Social | Concerns control over social interaction through geographical distance, group membership, and location. It is connected to physical privacy . | Ethics | Mittelstadt (2017[1]), Mittelstadt (2017[2]) |
| Application(GUI) | Acts as a component that controls and manages the transferred data to the server from the processing elements. [...] In order to resolve the lack of communication between patients and doctors in the current healthcare monitoring system | Website, Chat | Tan & Halim, (2019), Hu, et al. (2019), Azimi, et al., (2019) |

Source: Authors.

The components listed in Table 1 have been validated by specialists. The specialists are professionals with extensive market experience and who are currently dedicated to studying the IoT for approximately 5 years. They were organized in order to control the application risks in the health as represented in Figure 1.

**Figure 1**– Decomposition of the problem/decision.




Source: Authors.

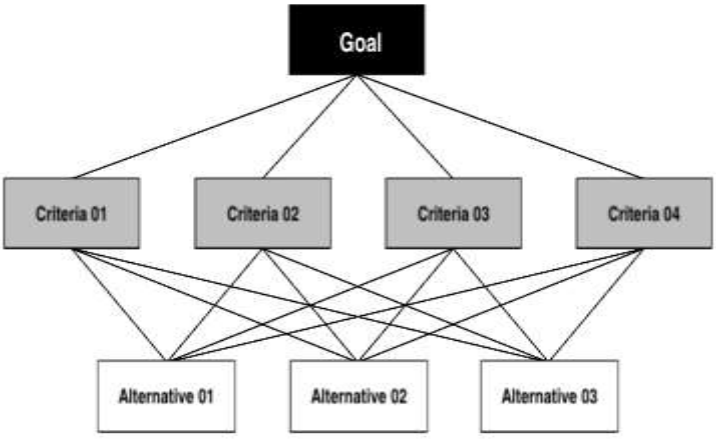
The risk problem in the IoT network was decomposed to help in the representation and assist in the control of the problem (Figure 1), for that the understanding of the components facilitates this activity. This understanding was detailed in Table 1.

**Application of AHP Method**

The Analytic Hierarchy Process provides a flexible and easy way to understand and analyze the risks of the study. It is a methodology of analysis of decision with several criteria that permit subjective and objective factors be considered in the process (Mustafa, 1991). Besides that, this is a general theory of evaluation largely accepted (Saaty, 2013).

The AHP application was divided into 3 (three) stages: decomposition of the problem in a hierarchy structure (Figure 2), arrangement of a comparing matrix among the criteria utilizing Saaty's importance scale (and respective normalization), calculation of the priority vector for the criteria (Saaty, 2008).

**Figure 2 –** AHP decision model.




Source: Authors.

The decomposition of a hierarchy of criteria is the representation of the goal, and association to possible criteria that composes it. So that, the goal is easily analyzable and the criteria is comparable independently.

From the decomposition of hierarchy process, the decision makers compare the criteria one by one to determine the relative importance between them and their relative influence to the global goal.

The comparison between two elements utilizing the AHP can be accomplished in several ways. However, the scale of relative importance between two elements proposed by Saaty (Saaty, 2008) is widely used, assigning values between 1 to 9. The scale determines the relative importance to an alternative in relation to the other, in conformity with Table 2.

**Table 2 –** Saaty´s scale importance.

| Scale | Numerical evaluation | Equivalent |
|---|---|---|
| **Extremely importance** | **9** | **1/9** |
| Very, very strong | 8 | 1/8 |
| **Very strong or demonstrated importance** | **7** | **1/7** |
| Strong plus | 6 | 1/6 |
| **Strong importance** | **5** | **1/5** |
| Moderate plus | 4 | 1/4 |
| **Moderate importance** | **3** | **1/3** |
| Weak or slight | 2 | 1/2 |
| **Equal importance** | **1** | **1** |

Generally, odd values are used, once the 2, 4, 6, 8 represent intermediate decisions. Source: Saaty (2008).

For the purpose of this study, this is the most appropriate method, as it can be partially implemented. This is consistent with the model proposed in this study, when decomposing the problem in a hierarchical structure until the systematic level of the criteria two by two. In addition, it allows the representation in a spreadsheet comparison matrix that makes easier the interaction with the specialist.

With the purpose of determining the contribution of each criteria/component to reach the global goal, it is necessary, firstly, the normalization of the comparison matrix and then the calculation of the priority vector or Eigen vector. The normalization is obtained by the division between each value of the spreadsheet with the total of each column, and the priority vector is obtained through the mean arithmetic of the normalized values of each of the criteria.

**Ranking Determination**

It is possible to define a ranking from the calculation of the priority vector, once it determines the contribution/influence of that criteria in the total result of the goal. The criteria with higher values in the priority vector took the top positions in the ranking, while the criteria with lower values in the priority vector took the last positions.

**Evaluation Rate Consistency**

Finally, the consistency index has to be evaluated (Saaty, 2013). The consistency index allows to verify if the result was representative and the grades were not assigned at random.

The index has the priority vector as basis and it is calculated through the sum of the result of each element of the vector by the total of the respective column of the original comparing matrix, being represented by $\lambda_{max}$.

Consistency level can be calculated, as follows:

$$CI = \frac{\lambda_{Max} - n}{n - 1},$$

where *CI* refers to the consistency index and n is the number of criteria.

The consistency rate (CR), can be obtained by dividing the consistency index by the random consistency index (RI), as follows:

$$CR = \frac{CI}{RI} < 0.1 \sim 10\%$$

where RI is obtained from Saaty (2013), as listed in Table 3. The pairwise comparison is considered consistent when CR is lower than 10%.

**Table 3 –** RI Values.

| **Num criteria (n)** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| **RI** | 0 | 0 | 0.58 | 0.9 | 1.12 | 1.24 | 1.32 | 1.41 | 1.45 | 1.49 |

Source: Saaty (2013).

**Numerical Application**

As mentioned in the previous topic, through Google Sheets, the comparing matrix were provided to the 2 (two) academic specialists to assign the weights. The criteria/components were organized in a matrix in order that each specialist could grade from 1 to 9. The grades were consolidated utilizing the geometric average and normalized in order to create a ranking, resulting in a comparison matrix (Table 4).

**Table 4 –** Comparison matrix.

| | **Device/ Sensor** | **Gateway** | **Algorithm** | **Protocol** | **Provider Services** | **Processing** | **Social** | **Application (GUI)** |
|---|---|---|---|---|---|---|---|---|
| **Device/ Sensor** | 1.00 | 3.87 | 1.73 | 1.73 | 2.24 | 1.73 | 7.94 | 3.87 |
| **Gateway** | 0.33 | 1.00 | 1.00 | 1.00 | 3.00 | 3.00 | 2.24 | 5.00 |
| **Algorithm** | 0.58 | 1.00 | 1.00 | 1.00 | 1.73 | 2.24 | 1.73 | 5.92 |
| **Protocol** | 0.58 | 1.00 | 1.00 | 1.00 | 1.73 | 1.73 | 3.87 | 1.73 |
| **Provider Services** | 0.45 | 0.33 | 0.58 | 0.58 | 1.00 | 3.87 | 1.73 | 2.24 |
| **Processing** | 0.58 | 0.33 | 0.45 | 0.58 | 0.26 | 1.00 | 1.73 | 1.73 |
| **Social** | 0.13 | 0.45 | 0.58 | 0.26 | 0.58 | 0.58 | 1.00 | 1.73 |
| **Application (GUI)** | 0.26 | 0.20 | 0.17 | 0.58 | 0.45 | 0.58 | 0.58 | 1.00 |
| **Total** | **3.90** | **8.19** | **6.50** | **6.72** | **10.98** | **14.73** | **20.82** | **23.22** |

Source: Authors.

With the purpose of better interpreting the data, the normalization was done dividing each value of the chart by the total of each column (Table 5).

**Table 5 –** Normalized matrix.

| | **Device/ Sensor** | **Gateway** | **Algorithm** | **Protocol** | **Provider Services** | **Processing** | **Social** | **Application (GUI)** |
|---|---|---|---|---|---|---|---|---|
| **Device/ Sensor** | 0.26 | 0.47 | 0.27 | 0.26 | 0.20 | 0.12 | 0.38 | 0.17 |
| **Gateway** | 0.09 | 0.12 | 0.15 | 0.15 | 0.27 | 0.20 | 0.11 | 0.22 |
| **Algorithm** | 0.15 | 0.12 | 0.15 | 0.15 | 0.16 | 0.15 | 0.08 | 0.25 |
| **Protocol** | 0.15 | 0.12 | 0.15 | 0.15 | 0.16 | 0.12 | 0.19 | 0.07 |
| **Provider Services** | 0.11 | 0.04 | 0.09 | 0.09 | 0.09 | 0.26 | 0.08 | 0.10 |
| **Processing** | 0.15 | 0.04 | 0.07 | 0.09 | 0.02 | 0.07 | 0.08 | 0.07 |
| **Social** | 0.03 | 0.05 | 0.09 | 0.04 | 0.05 | 0.04 | 0.05 | 0.07 |
| **Application (GUI)** | 0.07 | 0.02 | 0.03 | 0.09 | 0.04 | 0.04 | 0.03 | 0.04 |
| **Total** | **1.00** | **1.00** | **1.00** | **1.00** | **1.00** | **1.00** | **1.00** | **1.00** |

Source: Authors.

Finally, the priority vector it was calculated in order to find out the contribution of each criteria to control risks in the IoT network in the health area. This is obtained by arithmetic mean of the values of each criterion, creating a ranking (Table 6).

**Table 6 –** Priority Ranking.

| | **Priority Vector** | **Ranking** |
|---|---|---|
| **Device/ Sensor** | 0.27 | 1 |
| **Gateway** | 0.16 | 2 |
| **Algorithm** | 0.15 | 3 |
| **Protocol** | 0.14 | 4 |
| **Provider Services** | 0.11 | 5 |
| **Processing** | 0.07 | 6 |
| **Social** | 0.05 | 7 |
| **Application(GUI)** | 0.04 | 8 |

Source: Authors.

The next step was to calculate the consistency rate (CR) to check if the result was representative and the scores were not given at random. In the presented model, the RC is equal to 0.07, as shown in Table 7, thus the matrix can be considered consistent.

**Table 7 –** Rate consistency evaluation.

| Phase | Metric | Value | Formula/Comment |
|---|---|---|---|
| **1** | **Num Criteria** | 8.00 | |
| **2** | **ʎmax** | 8.70 | Adding the product of each element of the priority vector by the total of the respective column of the original comparing matrix |
| **3** | **RI tab** | 1.41 | Obtained in the chart of consistency index at random |
| **4** | **CI** | 0.10 | (ʎmax -n) / (n-1) |
| **5** | **RC** | **0.07** | (CI/RI tab) |

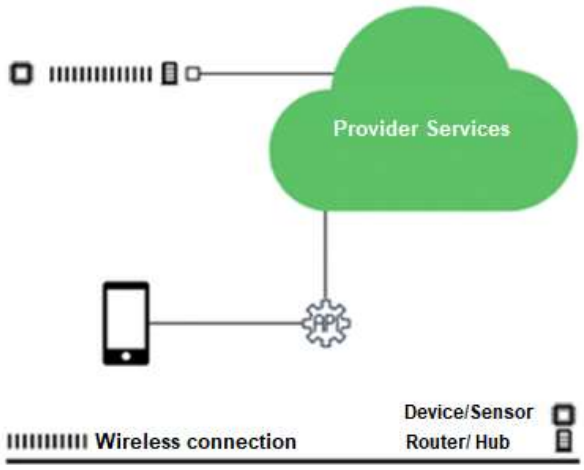
Source: Authors.

One can see that CR, from Table 7, is at the acceptable level (0.1 ~10%), with this the representative result is considered.

## 4. Discussion

In order to demonstrate the applicability of the proposed model, it was used to assess risk of a monitoring system for the refrigeration control of the magnetic resonance (MR) room (Bento, et al., 2019). The authors use the BMP085 sensor that can measure the temperature and atmospheric pressure and operated the 7-bit I2C protocol. The application codes were written in the C programming language and deployed in the cloud server and available by API (Application Programming Interface) technology. The complete connection scheme is illustrated in Figure 3.

**Figure 3 –** Connection scheme.




Source: Adapted from (Bento et. al, 2019)

In Figure 3 shows that all components extracted from the literature were applied to the proposed example, as well as the interaction between them.

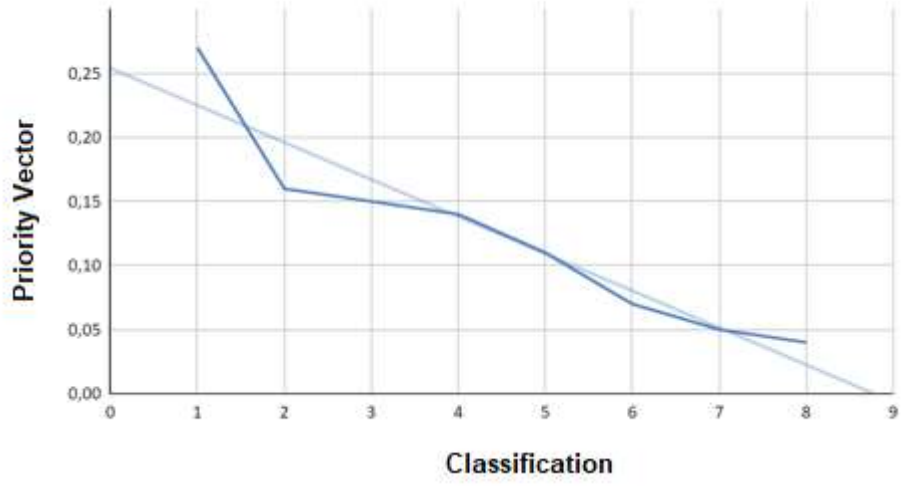
In this sense, the study resulted in a model that indicated the sensor for a high level of criticality highlighting the treatment of access control and data. At the same time, there was a low risk on the server side, as there are strict host policies. In addition, improvements were suggested in the implemented algorithms, such as checking the periodicity of data readings.

The use of new technologies, mainly in the health area presents complex challenges regarding the object of the experiment and the human being. The literature shows that the application of the IoT in the health area is promising, although there are challenges concerning the systems and technologies used. The numerical results show that they provide conditions to evaluate a risky situation involving the IoT measurement systems in the health area. The obtained RC (0.07) indicates that the

evaluated data are coherent among the experts' evaluation, which makes the application of the model viable According to the resulting priority vector (Table 7), where 1 has the greatest impact and 9 the least impact, the sensors (1) obtained a PV of 0.27, a value much bigger than the second (gateway) that was 0.11. The average distance between the PVs (2-9) is 0.2, which demonstrates the level of importance of the PV (1).

Figure 4 shows the existence of three priority groups, being formed by PV (1). PV (2,3,4,5) and PV (6,7,8). PV (1) is the starting point of the system, since data is collected in it and, due to this, it is the one that presents the greatest risk to the system and is under the vulnerabilities of the installation local. The second group includes VPs related to data transport, generally monitored by third parties, although there is the aspect of local security to access the components involved (transmission equipment, cabling, interface, among others). Finally, the latter group is responsible for processing and presenting the data. Although it belongs to this group, according to the classification of the VPs, the social aspect impacts on the issue of human presence, with regard to access to devices.

**Figure 4 –** Priority Vector X Classification.



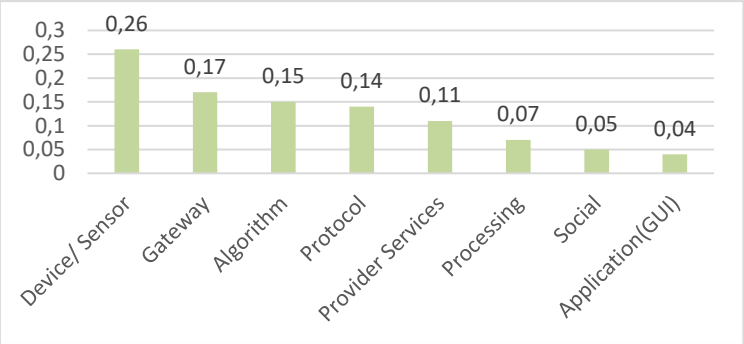

Source: Authors.

The utilization of the proposed risk assessment model provides conditions to assess and mitigate risks in applications that use the IoT within specific contexts in the health area. In other words, it follows ethical protocols and is in accordance with the case of application of the technology. The model includes applications described in the literature, which reinforces the question of its practical application. In many situations, the risks involved in the technological framework to implement the IoT are neglected, especially when using the standard parameters provided by manufacturers or models replicated in different environments. It is important to highlight that despite the elaboration of a risk exposure ranking, the IoT chain application in the health area demands a deep analysis on the other factors listed, as changes in the signal distribution (data) may occur if compared to the adopted standard. Thus, the proposed model allows a risk situation to be analyzed utilizing the elements included in the model.

Also, the literature review proposed a division of the IoT systems architecture into three groups. The first one refers to the devices/sensors (mobile and wearable sensors) that capture the patient and the context health data. The second group refers to the Gateway, which acts as a bridge between devices/sensors and the remote servers, being responsible for the data transmission and the protocol conversion. And the third one, the Provider Service, offers the transmission and data storage. It is also the means of offering health services, enabling the professionals to analyze and perform the diagnostics (Azimi, et al., 2019).

Mobile devices are seen as vital components to monitor patients and allow mobility. Furthermore, mobility allows to capture patient data in real time. This is one of the biggest benefits of applying the IoT in health. (Muhammed, et al., 2018). They are vital components. but vulnerable to installation locations, as mentioned previously. This can indicate the high impact on the model and the positioning in the ranking (Figure 5).

**Figure 5 –** Ranking of priorities vector.




Source: Authors.

There are few studies focusing on the receipt of data by health professionals or even social issues in the network. Among these studies, assessment/mitigation techniques are not applied. Probably, this may indicate that it cannot be controlled because it is an external factor. Regarding the ethical component, the IoT in the health field has to be designed to be technologically robust and scientifically reliable. Furthermore, it has to remain ethically responsible, reliable and respectful concerning the rights and interests of users (Mittelstadt, 2017).

## 5. Conclusion

The health sector is one of the first ones to adopt the Internet of Things (IoT). And, with the increase of wearables, health provider services are facilitated, offering economical cost of life such as real-time monitoring, vital reading, recommendations to healthy lifestyle and so on (Lomotey, et al. 2017).

This study proposed the application of the Analytic Hierarchy Process technique, resulting in a ranking of internal and external components that have higher impact on the network. From this ranking, it was verified that the Device/Sensor component represented the highest impact factor, indicating the necessity of closer attention by the decision maker in the mitigation of the risk. On the other hand, the Social and Application (GUI) were indicated components of lower impact in the IoT network.

The results pointed that the proposed AHP model can be used to assess criticality of the IoT components in different problems in the health area.

Moreover, the AHP technique allows to explore the problem in more hierarchy levels, by including alternatives, bringing, for instance, more details on the protocol vulnerability.

For further researches, alternatives could be included on the basis of this model, allowing to assess systems criticality and its application in other sectors could be investigated.

## Acknowledgements

This study was supported by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) and special thanks to Uninove for the scholarship.

## References

Albahri, O. S., Albahri, A. S., Zaidan, A. A., Zaidan, B. B., Alsalem, M. A., Mohsin, A. H., Mohammed, K. I., Alamoodi, A. H., Nidhal, S., Enaizan, O., Chyad, M. A., Abdulkareem, K. H., Almahdi, E. M., Al Shafeey, G. A., Baqer, M. J., Jasim, A. N., Jalood, N. S., & Shareef, A. H. (2019). Fault-Tolerant mHealth Framework in the Context of IoT Based Real-Time Wearable Health Data Sensors. *IEEE Access*. 7. 50052-50080. 10.1109/access.2019.2910411

Ali, F., Khand, P., Kwak, D., Islam, S. M., Ullahe, N., Yoo, S., & Kwak, K. S. (2018). Type-2 fuzzy ontology-aided recommendation systems for IoT-based healthcare. *Computer Communications*. 119. 138-155. 10.1016/j.comcom.2017.10.005.

Azimi, I., Pahikkala, T., Rahmani, A. M.., Niela-Vilén, H. Axelin, A., & Liljeberg, P. (2019). Missing data resilient decision-making for healthcare IoT through personalization: A case study on maternal health. *Future Generation Computer Systems*. 96. 297-308. 10.1016/j.future.2019.02.015

Ben-Daya, M., Hassini., E., & Bahroun, Z. (2017). Internet of things and supply chain management: a literature review. *International Journal of Production Research*. 57. (15-16). 4719-4742. 10.1080/00207543.2017.1402140

Biswas, A, & Giaffreda. R. (2014) IoT and cloud convergence: Opportunities and challenges. *IEEE World Forum on Internet of Things (WF-IoT)*. 375-376.

Bento, A., Gomes, J., & Melo de Souza, E., (2019) An IoT Experiment with Screen Development Using Nextion and ESP8266e + Motorshield. *10th International Conference on Computing*. Communication and Networking Technologies (ICCCNT).

Creswell. J. W., (2010). Projeto de pesquisa: Métodos qualitativo. Quantitativo e misto. Artmed.

Domingues, M. F., Alberto, N., Leitão, C. S. J., Tavares, C., De Lima, E. R., Radwan, A., Sucasas, V., Rodriguez, J., Andre, P. S. B., & Antunes, P. F. C. (2019). Insole Optical Fiber Sensor Architecture for Remote Gait Analysis-An e-Health Solution. *IEEE Internet of Things Journal*. 6 (1). 207-214. 10.1109/jiot.2017.2723263

Elsaadany, A., & Soliman, M. (2017). Experimental Evaluation of Internet of Things in the Educational Environment. *International Journal of Engineering Pedagogy*. 7 (3). 50-60. 10.3991/ijep.v7i3.7187

Gyamfi, K. S., Brusey, J., Gaura, E., & Wilkins, R. (2019). Heartbeat design for energy-aware IoT: Are your sensors alive?. *Expert Systems with Applications*. 128. 124-139. 10.1016/j.eswa.2019.03.022

Hu, Z. W., Bai Z. X., Yang, Y. Z., Zheng, Z. J., Bian, K. G., & Song L. Y. (2019). UAV Aided Aerial-Ground IoT for Air Quality Sensing in Smart City: Architecture. Technologies. and Implementation. *IEEE Network*. 33. 14-22. 10.1109/mnet.2019.1800214

Huang, Y. L., & Sun, W. L. (2018). An AHP-based Risk Assessment for an Industrial IoT Cloud. *18th IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. 637-638. 10.1109/qrs-c.2018.00112

Khan, T. A. Alam. M., Kadir. K. A Shahid. Z., & Mazliham. M. S. (2019). Artificial Intelligence based prediction of seizures for Epileptic Patients: IoT based Cost effective Solution. *7th International Conference on Information and Communication Technology (ICoICT)*. 10.1109/ICoICT.2019.8835350

Kumar, R. (2011). Research Methodology: a step-by-step guide for beginners. SAGE Publication.

Lomotey, R. K. Pry, J. & Sriramoju, S. (2017). Wearable IoT data stream traceability in a distributed health information system. *Pervasive and Mobile Computing*. 40. 692-707. 10.1016/j.pmcj.2017.06.020

Liao, Y. X., Deschamps, F., Loures. E., & Ramos, L. F. P. (2017) Past. present and future of Industry 4.0 - a systematic literature review and research agenda proposal. International *Journal of Production Research*. 55(12). 3609-3629. 10.1080/00207543.2017.1308576

Lin, Y. B., Lin, Y. W., Lin, J. Y., & Hung, H. N. (2019). SensorTalk: An IoT Device Failure Detection and Calibration Mechanism for Smart Farming. *Sensors*. 19 (21). 4788. 10.3390/s19214788

Mena, D. M., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A Global Perspective*. 27 (3). 162-182. 10.1080/19393555.2018.1458258

Mittelstadt, B. (2017). Ethics of the health-related internet of things: a narrative review. *Ethics and Information Technology*. 19 (3). 157-175. 10.1007/s10676-017-9426-4

Mittelstadt, B. (2017 [2]). Designing the health-related internet of things: Ethical principles and guidelines. *Information (Switzerland)*. 8 (3). 10.3390/info8030077

Muhammed, T., Mehmood, R., Albeshri. A., & Katib, I. (2018). UbeHealth: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities. *IEEE ACCESS*. 6. 10.1109 .32258-3285 /ACCESS.2018.2846609

Mustafa, M. A., & Albahar, J. (1991). Project risk assessment using the analytic hierarchy process.*IEEE Transactions on Engineering Management*. 38(1):46-52.1991. 10.1109/17.65759

Pereira, A. S. Shitsuka, D. M., Parreira, F. J., & Shitsuka, R. (2018). Metodologia da Pesquisa Científica. Universidade Federal de Santa Maria. (pp. 65-74).

Radanliev, P., De Roure, D. Nurse, J. R. C. Montalvo, R., Cannady, S., Santos, O., Maddox, La'Treall Burnap. P., & Maple, C. (2020). Future developments in cyber risk assessment for the internet of things. *SN Applied Sciences*. 2. 10.1007/s42452-019-1931-0

Ray, P. P., (2017). Understanding the role of internet of things towards smart e- healthcare services. *Biomed. Res*. 28 (4).1604–1609.

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*. 1(1). 83-98. 10.1504/ IJSSci.2008.01759.

Saaty, T. L. (2013). Theory and Applications of the Analytic Network Process: Decision Making with Benefits. Opportunities. Costs. and Risks. Pittsburgh: RWS Publications.

Sharma, S., Chen, K. & Sheth, A., (2018). Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. *IEEE Internet Computing*. 22 (2). 42-51.

Sood, S. K. & Mahajan, I. (2017). Wearable IoT sensor based healthcare system for identifying and controlling chikungunya virus. *Computers in Industry*. 91. 33-44. 10.1016/j.compind.2017.05.006

Tan, E., & Halim, Z. (2019). Health care Monitoring System and Analytics Based on Internet of Things Framework. *IETE JOURNAL OF RESEARCH*. 65 (5). 653-660. 10.1080/03772063.2018.1447402

Tao, H., Bhuiyan, M. Abdalla, A. N, Hassan M. M., Zain, J. M., & Hayajneh, T. (2019). Secured Data Collection with Hardware-Based Ciphers for IoT-Based Healthcare. *IEEE Internet of Things Journal*. 6 (1). 410-420. 10.1109/JIOT.2018.2854714

Wang, L. (2018). Environment supervision system for chemical industry park based on IOT. *Chemical Engineering Transactions*. 67. 481-486. 10.3303/CET1867081

Wilkerson, G. B. Gupta, A., & Colston. M. A. (2018). Mitigating Sports Injury Risks Using Internet of Things and Analytics Approaches. *Risk Analysis*. 38 (7). 1348-1360. 10.1111/risa.12984

Yan, B., Wang, X. & Shi, P. (2017). Risk assessment and control of agricultural supply chains under Internet of Things. *Agrekon - Agricultural Economics Research. Policy and Practice in Southern Africa*. 56 (1). 1-12. https://doi.org/10.1080/03031853.2017.1284680.