A Methodology for Trustworthy IoT in Healthcare-Related Environments

Lisa Pereira Michel[1], Carlos Lopes[2], Carlos Agostinho[2] and Raquel Melo de Almeida [3]

[1] *NOVA School of Science and Technology, Caparica, 2829-516, Portugal*
[2] *UNINOVA, Center of Technology and Systems (CTS), FCT-Campus, Caparica, 2829-516, Portugal*
[3] *Knowledgebiz Consulting, Rua Marcos Assunção 4, Almada, 2805-290, Portugal*

Abstract

The transition to the so-called retirement years comes with the freedom to pursue old passions and hobbies that were not possible to do in the past busy life. Unfortunately, that freedom does not come alone, as the previous young years are gone, and the body starts to feel the time that passed. The necessity to adapt elder way of living grows as they become more prone to health problems. Often, the solution for the attention required by the elders is nursing homes, or similar, that take away their so cherished independence. IoT has the great potential to help elder citizens stay healthier at home, since it has the possibility to connect and create non-intrusive systems capable of interpreting data and act accordingly. With that capability, comes the responsibility to ensure that the collected data is reliable and trustworthy, as human wellbeing may rely on it. Addressing this uncertainty is the motivation for the presented work. The proposed methodology to reduce this uncertainty and increase confidence relies on a data fusion and a redundancy approach, using a sensor set. Since the scope of wellbeing environment is wide, this paper focuses its proof of concept on the detection of falls inside home environments. The experimental results demonstrate that the solution implemented has more than 80% of reliable performance and can provide trustworthy results.

Keywords

Confidence metric, data fusion, healthcare

1. Introduction

The Internet was firstly created by people, for people and about people. It is one of the most important and transformative technologies ever invented. Nowadays, the Internet is not just about connecting people, but also connecting “things”. Devices that can sense, register data, and communicate with each other, as well as with the Internet, without the involvement of a human being. This new kind of internet it is called Internet of Things (IoT) and is generating huge amounts of information that can be used to create new ecosystems of business, industrial and consumer opportunities around data storage, analysis, and accessibility [1].

IoT devices can be used for medical and healthcare data collection and analysis, therefore the Internet of Medical Things (IoMT) has become a critical piece of the digital transformation of healthcare. For example, a smart home may be able to help keep elderly independent and remain longer in their homes, instead of going to nursing homes. Wearables can also bring several benefits as they collect health information of individuals in real time and activate alerts accordingly.

As IoT technology deals with sensitive personal data, trustworthiness is essential, especially when referring to the vision of trusting intelligent systems to make countless daily decisions that impact

Proceedings of the Workshop of I-ESA’22, March 23–24, 2022, Valencia, Spain
EMAIL: lisa.pmichel@gmail.com (L. Pereira Michel); csl@uninova.pt (C. Lopes); ca@uninova.pt (C. Agostinho); raquel.melo@knowledgebiz.pt (R. Melo de Almeida)
ORCID: 0000-0002-9002-7826 (L. Pereira Michel); 0000-0002-0972-7244 (C. Lopes); 0000-0002-2884-776X (C. Agostinho); 0000-0002-1049-453X (R. Melo de Almeida)
© 2022 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-3214/WS7Paper1.pdf

human lives [2]. False alarms (when systems signal an alarm that afterwards is proven unfounded), and misses (occur when the system fails to recognize the situation that is supposed to trigger the alarm) influence the level of trust in the automated system, particularly on compliance/reliance behaviours. Meaning that, after multiple false alarms, the tendency is to delay the response to the system alarm, or even ignore it, reducing the system compliance. Whereas the effect of misses leads to an increase of human control over the system, reducing its reliance [3].

As mentioned, it is very important to have a reliable and trustworthy system when dealing with sensitive data. This paper tries to precisely improve the data reliability, therefore increasing the confidence in an IoT system for older citizens, so that they can live a more independent and happier life.

2. Related work

With this chapter an introductory overview of the most important concepts supporting this paper is presented. The core objective of this background research is to form a consisting base support necessary for the implementation and accomplishment of the proposed solution for the problem identified.

2.1. Sensor fusion

To improve accuracy and avoid misclassifications, multisensory techniques can be employed in a way that it is hardly performed by the same set of sensors working separately. Data fusion is a multi-disciplinary research area that uses knowledge from many diverse fields, such as signal processing, information theory, and artificial intelligence [4]. The concept is present everywhere, for example, to evaluate a wine, a sommelier, does not only use his taste, but also his vision and sense of smell.

In [5], there is a combination of different technologies to increase the performance and reliability of the system, and therefore the increase of trust in the system. The information provided by an accelerometer and a gyroscope is used to improve the classification performance, by reducing misclassifications, specifically false positives and consequently false alarms.

The information collected by the sensors, about the user posture, is periodically transmitted to a centralized monitoring system, where a cross correlation is computed. If the correlation exceeds the predefined threshold, the event is classified as potentially belonging to a specific class. When a critical event is detected, the system immediately alerts the caregiver, by an event triggered transmission protocol.

2.2. Fault handling

IoT systems are employed in diverse environments leading to failures caused by issues such as user error, flaws in the device hardware and software, weather, etc [6]. Either in the form of managing anomalies or eliminating uncertainties, it is interesting to analyse how one can overcome such situation to build a more trustworthy system.

In [7] it is proposed a new feature-based learning system to classify data and detect anomaly events effectively. They use a neural network composed of Radial Basis Function (RBF) and Backpropagation (BP) networks as shown in Figure 1.

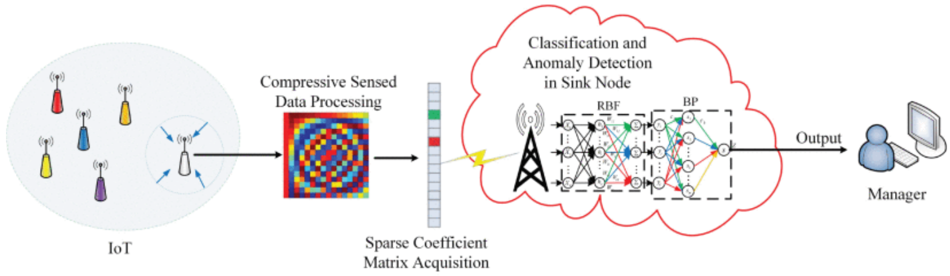

Figure 1: Data classification and anomaly detection [7]

As illustrated, the process to classify sensor data occurs in the sink node, which acquires the common sparse coefficient matrix and unique sparse coefficient and then identifies data classes according to the historical data. The trained RBF-BP hybrid neural network detects anomalies in the sensor data and obtains the state anomaly probabilities. By analysing the correlation between the sensor data with the RBF, the state anomaly probability of things can be acquired for the user to make timely decisions. By providing this anomaly probability, the system gives a sense of confidence, because then the user is properly informed about the state of the system data. It is a visualization approach so that the user can better informed decisions.

2.3. Event classification

Artificial Intelligence (AI) can observe and analyze several features in order to detect events that are interesting for the system application. When the event is detected, it is categorized and can be used to trigger further actions. For example, a smart coffee machine that is turned on when it detects that its user has woken up, or a house that is unlocked by detecting its owner voice.

AI platforms that provide event classification techniques are heavily searched in the IoT world. One example is the Tensor Flow open-source platform, where its users can develop and train machine learning models. With these models it is possible to classify images, sounds events, speech recognition, text classification, etc. Numerous applications, especially healthcare ones, can be developed by these techniques.

From all the presented concepts, data fusion, which integrates multiple data sources, fault handling, which deals with a system failure, and event classification are the techniques more suitable to accomplish the proposed solution for the problem identified, as discussed in the following chapter.

3. Methodology for trustworthy IoT

The proposed solution is to design and implement a methodology for trustworthy IoT based in redundancy operations. Introducing redundancy in the system without compromising its performance, allows to enhance the quality of results by a more reliable IoT process that ultimately leads to more accurate results. Therefore, the purpose of the system can be met with an increased degree of confidence, which is a concept inspired by the background research and is associated with each detected event. In Figure 2 it is possible to observe the methodology adopted in this work.

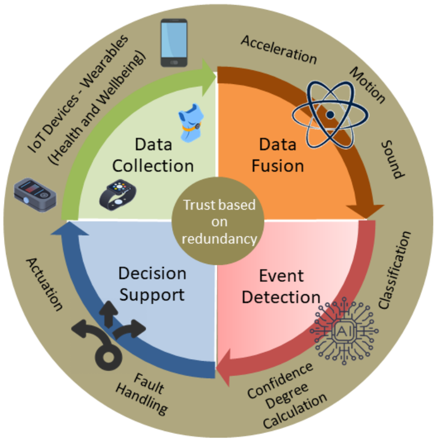

Figure 2: Conceptual Methodology

Redundancy is present in each phase of the methodology which is described as follows:

- Data collection: redundancy is ensured by having different types of sensors as data sources. For this purpose, in a healthcare environment, wearables with complementary data are used, such as smartwatches, smart shoes, smart glasses, etc.
- Data fusion: since there are different types of sensors as data sources, there are different types of data to be processed and analysed. Motion, steps, or audio data can be combined to create redundancy because they describe the same event in different ways.
- Event detection: in the methodology designed, the event classification produces an outcome (degree of confidence) that depends on the combination of the different data sources. Actions will be triggered depending on the degree of confidence value.
- Decision support: the presented methodology has a fault handling technique, which confirms if the event detected is correctly classified, with this being another form of redundancy. Depending on the fault-handling outcome, further actions are taken as a form of decision support.

In conclusion, to ensure the maximum trust on a IoT system, there should be a number of redundant data sources for a meaningful data fusion and a proper event classification with a significant degree of confidence calculated.

3.1. Methodology workflow

The methodology presented earlier is generic enough for any IoT-based scenario. As healthcare is a large domain with many applications of interest, this paper selected a fall detection scenario to instantiate the methodology. The diagram of Figure 3 represents the behavior of a IoT system, with multiple data sources.

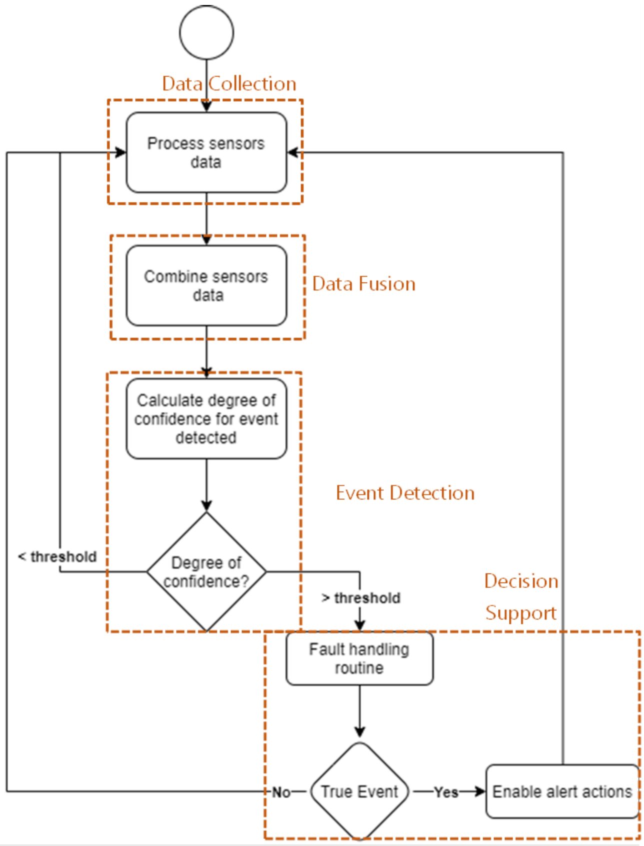

Figure 3: Methodology workflow

To start, the system must be operational, therefore the sensors need to be enabled and connected. The selected sensors might need a Bluetooth connection to send its data, or another protocol activated, so the processing unit needs to apply the Bluetooth Low Energy (BLE) protocol, as well as any other common protocols needed.

After that, the system is ready to receive, process and combine the sensors data. The outcome of that fusion allows the calculation of a degree of confidence that, depending on its value, enables a fault handling technique. If the fault handling routine concludes that a relevant event has indeed happened (true event), it activates alert actions and afterwards continues processing sensor data. If the fault routine declares that a relevant event did not happen (false event), then the system does not bother the user and continues processing sensor data.

The false alarms and misses events were the focus of the presented work when developing the methodology, which concluded that a system needs a data fusion from more than one redundant or complementary data sources, to properly classify a detected event and have a validation technique to confirm that event.

To bring the different types of data together and classify an event detected it is necessary to have a common "language" that translates the information received. For that, a confidence degree was developed.

The confidence level is a percentage value that represents how reliable the system is in classifying the event detected. Its value depends on the combined information received by the system's data sources. The principle is, the greater the number of events detected, from the different data sources, the greater the degree of confidence and therefore the greater the confidence in the system. If the values received from one sensor indicate that an event has occurred (a possible fall), the system combines the values received from all the sensors and calculates the degree of confidence. If the values from all the sensors indicate that a fall has occurred, the degree of confidence will be higher than if only one sensor indicates that a fall has occurred. In this way, the system uses redundancy by confirming an event detected by one sensor with values from the other sensor(s).

To have a more complete and reliable confidence degree method, the system should also have a timeframe that allows all relevant events detected to contribute to the confidence degree within that timeframe. This means that a relevant event detected affects the confidence degree for a certain period of time.

The confidence degree calculation also serves as a condition to trigger the fault handling routine that can take many forms, it can be a button that if pressed it confirms the detected event. Either way, this redundancy approach is necessary to increase even more the system reliability and therefore the trust on the system.

The fault handling routine is also a condition to trigger the next actions that notify the user for the event detected. In addition to notifying the user of what has happened and indicating the recommended next steps, it is also interesting to show the degree of confidence so that the user can make the most informed decision possible.

4. Implementation and test results

This chapter discusses the implementation of the fall detection phone app developed, that uses the methodology explained in the previous chapter. The name of the app is Fall Fusion, and it was developed in the Android Studio tool.

4.1. Implementation details

In the designed solution, there are two different types of input data: motion and audio. This choice of data was made because a fall is characterized by a rapid and uncontrolled movement often accompanied by a sound coming from the fallen person or/and an object hitting a surface. For the motion data, the system uses a 3-axis accelerometer integrated in a wearable sensor and a threshold method is used to detect a possible fall. For the audio data, a smartphone microphone serves the purpose because it will be used both as a sensor and as a processing unit. A machine learning model from the Tensor Flow platform was used to identify certain sounds that evidence a possible fall event.

The confidence degree is a value between 0 and 100 and is obtained as follow:

$$Confidence\ Degree = 0.7 \times motionTrust + 0.3 \times audioTrust \tag{1}$$

Because a fall is mainly a motion event the accelerometer has a bigger importance than the microphone, therefore he will have a greater weight in the event confidence degree. This means that if the accelerometer detects a possible fall, the system will enable the alert actions process regardless if the microphone detected something or not. The accelerometer priority does not cancel out the importance of the audio, because the confidence degree will be higher if both the accelerometer and the microphone detect a fall, compared to the accelerometer being the only one to detect it.

After the confidence degree calculation, its value is checked and if it is greater than 20, which is the threshold defined after several experiments, a fault handling routine is triggered. The fault handling routine is deployed by printing a button on the smartphone screen. If the user does not click it within a certain period of time an e-mail will be sent to their emergency contact. The message information changes according to the type of event detected (audio and/or movement) and if the user pressed the button.

4.2. Results and discussion

The performance of the proposed system is evaluated with 7 types of daily activities and one fall event. Each activity was performed 10 times, making a total of 70 sample tests that involved movement and/or sound.

Some of the audio samples used were from the collection of sound clips drawn from YouTube, available on Audio Set from Google.

The experiments have four possible outcomes:

- True positive (TP) is defined as an event that the system detected a fall when a fall has happened.

- False negative (FN) is defined as an event that the system did not detect a fall when a fall has happened.
- True negative (TN) is defined as an event that the system did not detect a fall when a fall did not happen.
- False positive (FP) is defined as an event that the system detected a fall when a fall did not happen.

The system performance is calculated as follow:

$$System\ Performance = \frac{TP + TN}{Total\ Experiments} \times 100 \tag{2}$$

The results of the experimental data are shown in Table 1. By applying Equation 2 to the results, the system performance has a value of 83%, which is a good starting point for a prototype.

Table 1
Proposed system performance

Activities experiments	Number of experiments	True positive (TP)	False negative (FN)	True negative (TN)	False positive (FP)	Performance	System Performance
Falling	10	7	3			70%	83%
Sitting/Getting up	10			7	3	70%	
Laying down	10			8	2	80%	
Walking	10			10		100%	
Going downstairs	10			7	3	70%	
Doing the dishes	10			10		100%	
Watching Tv	10			9	1	90%	
Total	**70**	**7**	**3**	**51**	**9**		

A total of 7 out of 10 falls were detected and 3 of the falls were not detected because the confidence degree was not higher than the threshold. This may have been because the fall was very soft, or because no sound was heard evidencing a fall.

It is important to mention that most of the fall's experiments were correctly detected due to the motion sensor, even though sounds were also played. This means that the system recognizes a dangerous movement better than an alarming sound. This does not compromise the system as the alert button creates extra redundancy in the system and all detected events are presented to the emergency contact so he can make the most informed decision possible.

5. Conclusion

The motivation for the present study was the potential that IoT systems can create in today's society. Especially in the older population, as they are more susceptible to debilitating conditions. For this reason, it is vital to continuously bring new forms of technology that enable a more independent and healthy life.

Beside the technology development, it is tremendously important to increase the use of it, which is often linked to concerns and doubts created by situations like false or missed alarms. It was precisely this mistrust that this study tried to solve or at least diminish.

The methodology presented is a system with a number of redundant data sources for a meaningful data fusion and a proper event classification with a significant degree of confidence calculated. Where the degree of confidence technique was the innovative work approach, which is the percentage value that represents the reliability the system has on the event detected classification. Its value depends on the combined information received by the system's data sources. The principle is, the higher events number detected, from the different data sources, the higher is the degree of confidence and, therefore, higher is the trust on the system.

As healthcare is a large domain with many applications of interest, this study focused on the detection of falls, inside home environments. Hence, a fall detection phone application using sensor fusion and methods to create extra redundancy was developed. The data sources chosen were from a smartphone microphone (audio) and from an accelerometer (motion) sensor embedded in a wearable. This choice of sensor combination being also innovative, considering the current offer of sensors present in a fall detection system.

The tests results show that the system has a performance of 83% and the detection of more than one event by both or one of the sensors has a higher degree of confidence than if it was one event detected. This proves that having a number of redundant data sources for a meaningful data fusion improves the system reliability and therefore the trust on the system, as foreseen in the work hypothesis.

It would be interesting to further develop the concepts of event synchronism and database in the conceptual methodology, in a sense of creating an history of events that could be accessed and weighted in the fused data.

As future work, the system performance could be increased by training the machine learning audio classifier more and by turning the system cross platform, being accessible also in iOS applications.

Regarding the system workflow, an improvement could be a buzzer that alerted the user in case the Bluetooth connection was lost. A buzzer to catch the user attention to the alert button could also be an improvement, as well as alert messages sent to the emergency con-tact's mobile phone instead of the email.

6. Acknowledgments

This work has been developed in the context of Smart4Health project. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 826117.

7. References

[1] J. M. Wilson, A. McKinlay, Rethinking the assembly line: Organisation, performance and productivity in Ford Motor Company, c. 1908-27, Business History 52 (2010) 760-778. doi: 10.1080/00076791.2010.499425.

[2] R. Melo-Almeida, C. Agostinho, R. Jardim-Goncalves, A self sustainable approach for IoT services provisioning, in: K. Mertins, R. Jardim-Goncalves, K. Popplewell, J. P. Mendonca (Eds.), Enterprise Interoperability VII. Enterprise Interoperability in the Digitalized and Networked Factory of the Future, Springer, Cham, 2018, pp. 39–50, doi: 10.1007/978-3-319-30957-6_4.

[3] E. T. Chancey, J. P. Bliss, Y. Yamani, H. A. H. Handley, Trust and the Compliance-Reliance Paradigm: The Effects of Risk, Error Bias, and Reliability on Trust and Dependence, Human Factors: The Journal of the Human Factors and Ergonomics Society 59 (2017) 333-345. doi: 10.1177/0018720816682648.

[4] B. Khaleghi, A. Khamis, F. O. Karray, S. N. Razavi, Corrigendum to ‘Multisensor data fusion: A review of the state-of-the-art’, Information Fusion 14 (2013) 562. doi: 10.1016/j.inffus.2012.10.004.

[5] B. Ando, S. Baglio, C. O. Lombardo, V. Marletta, A multisensor data-fusion approach for ADL and fall classification, IEEE Transactions on Instrumentation and Measurement 65 (2016) 1960–1967. doi: 10.1109/TIM.2016.2552678.

[6] M. Norris, B. Celik, P. Venkatesh, S. Zhao, P. McDaniel, A. Sivasubramaniam, G. Tan, IoTRepair: Systematically addressing device faults in commodity IoT, in: Proceedings - 5th ACM/IEEE Conference on Internet of Things Design and Implementation, IoTDI 2020, IEEE, New York, 2020, pp. 142–148, doi: 10.1109/IoTDI49375.2020.00021.

[7] D. Wu, H. Shi, H. Wang, R. Wang, H. Fang, A feature-based learning system for internet of

things applications, IEEE Internet of Things Journal 6 (2019) 1928–1937. doi: 10.1109/JIOT.2018.2884485.