Towards a Trustworthy Patient Home-Care thanks to an Edge-Node Infrastructure

Carmelo Ardito[1], Tommaso Di Noia[1], Eugenio Di Sciascio[1], Domenico Lofù[1,2], Giulio Mallardi[1,2], Claudio Pomo[1], and Felice Vitulano[2]

[1] Politecnico di Bari – Via E. Orabona 4, Bari (I-70125), Italy {carmelo.ardito, tommaso.dinoia, eugenio.disciascio, domenico.lofu, giulio.mallardi, claudio.pomo}@poliba.it

[2] Innovation Lab, Exprivia S.p.A. – Via A. Olivetti 11, Molfetta (I-70056), Italy {domenico.lofu, giulio.mallardi, felice.vitulano}@exprivia.com

Abstract. Ambient Assisted Living (AAL) promotes the assistance of a patient at home according to her/his Clinical Pathway, i.e., a set of diagnostic and therapeutic procedures related to the treatment of that specific patient. AAL is increasingly gaining momentum thanks to the Internet of Things (IoT). Edge-Computing would boost the AAL success, since this kind of architecture promotes a sort of distributed cloud computing at the edges of the IoT network, thus reducing latency and improving reliability. This poster paper focuses on the implementation, in a AAL system based on such an IoT-Edge-Computing coupled architecture, of an anomaly detection module able to detect deviations from the patient's Clinical Pathway (CP) and avoid processing of inconsistent or fake data, which could result in a serious life-threatening for a patient.

Keywords: Anomaly Detection · Edge-Computing · Smart Healthcare.

1 Introduction

It has been clear for several years now that, in order to reduce healthcare costs, it is important to leverage the possibilities offered by Ambient Assisted Living (AAL) for home care of patients. In addition, the recent COVID-19 emergency has also shown how, in order to mitigate the spread of the contagion, it is necessary to minimise access to hospital facilities by those chronically ill patients who can be monitored at home. And even COVID patients with mild symptoms can be cared for remotely, without the need to take up hospital places that can be allocated to more severe patients and without the risk of worsening their situation due to contact with the latter.

The adoption of Clinical Pathways CPs [7] [14] would make AAL implementations much more effective, as it would allow remote monitoring of patient care and automate the reporting of critical events that deviate from the prescribed care, also thanks to the use of Machine Learning techniques. A CP consists of a set of diagnostic and therapeutic procedures. It can be considered as a

process model characterized by two main phases: (i) some activities, or sub-processes, that can be managed by the personnel in the health structures; and (ii) some others that can be managed autonomously by the patient, in a sort of medical-unsupervised manner. The latter phase can be processed by an intelligent architecture able to deal with the specific clinical sub-path for the patient at home, also checking that is validated by a doctor or nurse, and guaranteeing its compliance with the actual medical indications specified in the clinical path.

AAL is becoming more and more successful thanks to the evolution of IoT technology and in particular of wearable devices. However, it must be considered that there are limits, mainly due to the latency of the network, that sometimes make the use of such solutions critical in the healthcare. The security of data being transmitted from sensors to the cloud is another area of concern, as their transmission could be affected either by technical problems or by malicious manipulations, in both cases resulting in life-threatening for the patient. Sensitive patient's information could also be sniffed.

In order to address these issues, the proposal in this Late Breaking Result paper consists of an architecture that couples IoT and Edge-Computing, which also implements an anomaly detection module able to detect deviations from the patient's CP.

Moreover, exploiting Edge-Computing in this approach, the privacy preserving requirements are embraced implicitly due to nature of this sort of distributed architecture.

2 Related Work

With the advent of IoT, monitoring patients' care and their vital parameters has become easier thanks to wearable devices. Still, there are issues related to performances and security.

Weareable IoT devices are applied in crucial applications: monitoring vital signs, tracking indoor positions, or alerting for some crucial events [5]. Besides, with the advent of machine learning, these applications are becoming more and more sophisticated, requiring much computational power. Processes driven by such devices become time-consuming and harvest much computational power, thus also impacting on the battery life.

Low latency to send and receive critical data or high reliability to scale or replace these devices are the most critical constraints in the healthcare context. Standard cloud architectures to manage the network communications cannot be exploited. Indeed, cloud computing is not designed with these goals in mind, thus it doesn't fulfil these requirements [2].

The Multi-access Edge Computing (MEC) approach addresses this issue [16] [2]. MEC is defined as the ability to process and store data at the edge of the network, i.e., in the proximity of the data sources. By adopting this architecture, bottlenecks in healthcare systems can be significantly reduced thanks to the less amount of data transferred to the cloud. MEC's advantage in a smart health environment is multifaceted, as it can provide short response time, decreased

energy consumption for battery-operated devices, network bandwidth saving, secure transmission and data privacy [1].
Edge computing is a promising solution to mitigate this issue. It is distributed, thus sensible data are pre-processed on the edge of the network and obfuscated sensitive information of the patient are sent to a central server that needs only extracted features to perform related tasks.

However, these smart devices can also be subject to malfunctions and technical anomalies (intentional or unintentional). It is fundamental to detect in order to avoid serious life-threatening for a patient.

An anomaly detection system is proposed in [10]. It is based on the extraction of care-flow records that regularly capture medical behaviors in clinical processes, also identifying the anomalous ones. In order to monitor patient treatment and care behaviors in a variety of clinical settings, this approach requires an high-frequency detection rate of the care-flow records and a specific description of them.

Ahsanul Haque et al. [9] present a system for the detection of sensor anomalies in healthcare, able to distinguish real alarms from false alarms. The system is implemented in Java combined to WEKA framework. The system was tested on three real medical datasets. The value detected by a sensor is compared with the historical data, in order to detect suspicious variations. The experimental results show a Detection Rate (DR) of 100 % and a low false-positive rate (FPR) for all the datasets.

Unfortunately, none of the solutions presented above fully meets the key requirements and challenges in the field of anomaly and attack detection in healthcare. The system proposed in this paper aims at offering a complete, autonomous, and effective architecture, which is also able to detect anomalies and cyber attacks in the healthcare domain.

3 System Architecture

The proposed system, thanks to the use of Bluetooth sensors, is able to monitor clinical parameters without the need of the physical presence of a healthcare professional. The system detects various clinical parameters (e.g., Blood Oxygen Level (OXI), Electrocardiogram (ECG), body temperature, etc.), processes captured data and generates the Clinical Pathway for the patient under treatment. This approach is a common strategy in this scenario; like depicted in [2] [5] collecting remote data from these sensors will be more complex due to the heterogeneous devices involved in measurement of these parameters.

Figure 1 depicts a general overview of the system architecture for the continuous monitoring of a patient and safe management of his/her CP. Each smart device (e.g. headband, smartwatch) feeds the Infrastructure Edge Node with its specific data. Thanks to machine learning solutions and related e-health techniques, these data are used to monitor a patient and produce an efficient clinical path, give continuous feedback about health conditions to the doctor's control unit and enable interaction between doctor, patient, and his/her relatives.

The data management is a challenging aspect because of the ingestion of heterogeneous data with low latency and zero downtime, alongside the generation of a proper clinical Pathway based on patient history. These crucial aspects are linked to some other issues: one of the most critical is the anomaly detection.

The core of the architecture is a cluster of edge nodes that cooperate to perform a sort of Extract, transform, load (ETL) task. This cluster is intrinsically linked to the anomaly detection and it matches the constraints of MEC solution proposed by [16], which monitors the general task step by step. The main

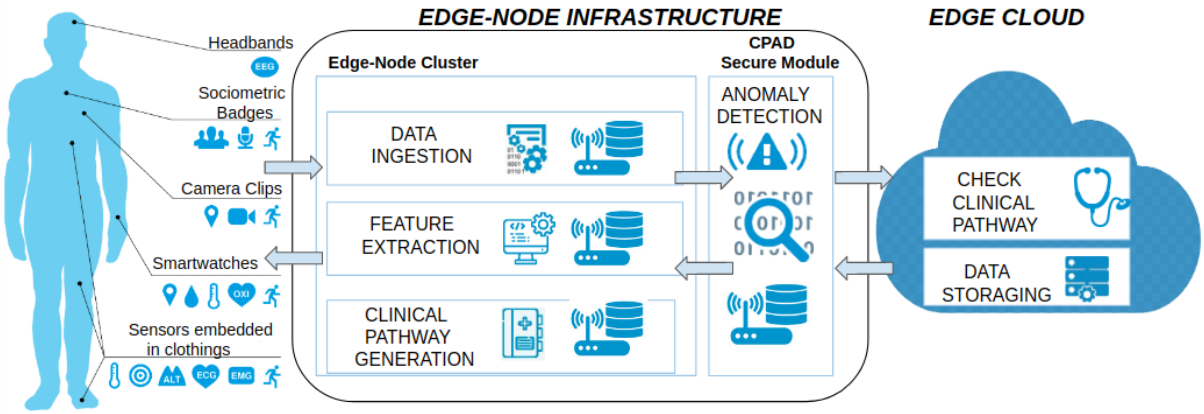

Fig. 1. The Proposed Architecture.

components of the architecture are described in the following.

Data Ingestion node. As stressed before, due to the massive employment of various smart devices, a data ingestion module orchestrates all data streams coming from these objects. This node is devoted to creating links between wearable medical devices and other modules belonging to the architecture. Data flows are injected into the Feature Extraction node for further specific elaborations and in the Clinical Path Anomaly Detection node to identify malformed data.

Feature Extraction node. One of the most critical issues to address is to guarantee the data privacy of each patient. For this reason, data flow coming from smart medical devices are processed at the edge of the network by this node. All vital sign data are analyzed to extract notable characteristics from the stream. These features are then injected into the Clinical Path Anomaly Detection module to be confident about the goodness of the detected data or to identify some troubles inside them.

Clinical Pathway Generation node. Among the goals of the system, the generation of a personalized clinical pathway is a crucial task. The approach adopted in Mallardi et al. [4] is growing up as the main instrument for the implementation of clinical guidelines and evidence-based medicine.

Thanks to this node, the system learns from patient's history and combine this knowledge with that provided by doctors, thus producing a tailored therapy. Also this node interacts with the Clinical Path Anomaly Detection module to identify possible issues.

Clinical Path Anomaly Detection (CPAD) module. The specific design of this module, which represents the main contribution here, is detailed in the next section. This module makes the system less prone to anomalous situations, such as: (i) a specific malfunction related to vital sign and the therapy specified in the clinical pathway, (ii) hardware fail situations like battery degradation, (iii) system hacking by the patient or data tampering by someone not authorized to be involved in this process.

Edge Cloud. With this component, it is possible to manage two specific aspects of this scenario. First, it is possible to store all the data coming from the single edge-node cluster in a privacy-aware manner. Recently, this kind of approach has emerged as a common solution in the IoT ecosystem with specific constraints, like in the health domain. In [16] these constraints are matched in MEC Architecture. Then, for every CP generated by the Clinical Pathway Generation module, a specific component performs a formal check for possible inconsistencies.

4 Clinical Path Anomaly Detection Secure Module

Anomaly detection is of pivotal interest not only in network intrusion detection [6], fraud detection in financial domain [3], air pollution [15], but also in the healthcare domain concerning medical diagnosis [17].

As state in Section 3, sensors detect the vital parameters and send them at the Edge-Node cluster where the *Ingestion* node performs data orchestration. Then, the *Feature Extraction* node extracts key features. To check if data transmission is correct and that there have been no malfunctions (including system hacking), the proposed system is equipped with a module called *Clinical Path Anomaly Detection (CPAD).*

The CPAD module analyzes all the data transmitted from the devices monitoring the patient to the Edge-Node cluster and eventually notifies detected anomalies.

The CPAD module, using specifically implemented machine learning techniques, manages the security issues that could occur during the data transmission process. In this context the anomaly could also consist of an attack to the monitoring of the patient's clinical parameters. The detected anomaly causes a dysfunction in the CP that in turn has a direct impact on the patient's health.

4.1 Technological Approach

The data collected in the *Ingestion* node can be seen as a queue and as organized into several sub-processes. Each sub-process represents the detection phase of a vital parameter from a single device worn by the patient. Thanks to the adoption of a recurrent sequential Long Short Term Memory (LSTM) autoencoder, the CPAD analyzes the various sub-processes of the chain to perform the detection of anomalies on the steps of the chain [11] [12].

In particular, the advantage of using sequential LSTM autoencoders is twofold: (i) taking advantage of the dimensionality reduction and extraction capabilities of the autoencoder to efficiently perform the data reconstruction process, and then detect the anomaly and (ii) using LSTM networks to manage the sequential nature of the data detected by the sensors.

The difference between a regular and recurrent autoencoders may be summarised as it follows: regular autoencoders work on sequential data by fixing the data size, usually by padding all sequences with zero vectors to the length of the longest sequence [13]. In contrast, the recurrent autoencoders that were adopted in this proposal can compress variable-length sequences into fixed-length representations [8]. Therefore, they can generalize dependencies between nearby frames to other positions in the sequence.

In this way, the CPAD Module is able to define whether or not the patient's CP is correct. Otherwise, a specific machine learning algorithm adjusts the CPs according to the data currently detected. The CPAD Module is able to detect three types of anomalies:

1. **Specific Malfunction**: it indicates a specific system malfunction. The module can detect whether the parameters that are transmitted from wearable devices to the edge node are reliable or not. It is also able to monitor whether the actions to be performed are those as per the CP.
2. **Hardware Malfunction**: it indicates a hardware malfunction. The module can detect the battery-charge status of the devices and the malfunctioning of the detection probes and patches. It also detects transmission errors at the Bluetooth protocol level.
3. **System Hacking**: it indicates system hacking. The module can detect if someone is trying to hack the system and if the user is trying to trick them.

4.2 Running Example

Suppose that the system is used to monitor a patient's in-home care. The patient suffers from a particular pathology that, among other problems, causes high blood pressure. To be able to lower the pressure, the doctor has prescribed two pressure pills a day, one at 07.00 am and the other at 09.00 pm. The doctor's diagnosis and the prescriptions for the medications to be taken are part of the CP. The pills are in a smart container (e.g. RxCap [3]) which indicates the time at which a pill is taken. If the doctor has prescribed that the patient should only take the pill twice a day, the CP knows that the sensor that controls the opening of the container should only be opened (or closed) twice a day and the pill can only be taken twice. The sphygmomanometer worn by the patient, according to the pressure monitoring instructions of the CP, performs pressure monitoring 5 times a day: 06.00 am, 09.00 am, 03.00 pm, 05.00 pm, and 08.00 pm. If the value of the pressure measurement is not in the range indicated in the CP, the CPAD detects a *Specific Malfunction*. This generates a notification that informs the

[3] https://rxcap.com/

actors involved (doctor, patient and relatives) of this event, and the correction flows are then appropriately generated.

It is possible to know the behavior of each sensor because the hardware specifications and operating details (and also malfunctioning) are available. For example, the sphygmomanometer measures blood pressure at predefined intervals, as specified in the CP. The pressure measurement process takes 30 seconds. If the measurement process lasted only 10 seconds, it detects a *Hardware Malfunction*, which is due to several factors, e.g. low battery.

In the same scenario, an example of *System Hacking* is the following one: the doctor has prescribed two blood pressure pills a day. This information is codified in the CP, thus it is displayed on the patient's tablet or programmed in the pill dispenser. The system could be hacked so that the number of pills is increased to 4.

5 Discussion and Conclusion

The main contribution of this poster paper is about the Edge-Node architecture and its capability of detecting different kinds of anomalies in the healthcare domain, which could be useful in particular for patient assisted at home. This approach exploits a novel machine learning technique, implemented in the CPAD module, that encapsulates two layers of LSTM into an Autoencoder structure. Indeed, the overall idea is to detect and keep track of anomaly situations with respect to the clinical history of a patient.

An interesting factor to address for future development is a module that acts as an "explainer". The explanation of artificial intelligence is a critical aspect in all the system that supports human decisions, and also this scenario could be examined from this point of view. This aspect represents a conjunction of different spheres: from the classical side of philosophical details to human-computer interaction. An extensive scientific literature corpus supports the importance of the explanation in this kind of systems. It could be fascinating to examine this aspect in the proposed approach to measure how various actors of the domain perceive system decisions.

This aspect is strictly linked to the users' trustability in the system. This is particular important in the the healthcare domain, since it involves crucial aspects of people's life. For example, suppose that a patient is used to take a pill to control blood pressure twice a day. If some vital parameters involved in his/her pathology go out of a determined range, the Clinical Pathway Generator module could proactively react and change the pathway, asking the patient to to take one more pill. How could the patient be serene that the modification does not depend on a malfunction? It is interesting to explore how visual explanations can improve system trustability. Nevertheless, such smart devices could have a peculiar trustability, eventually equipped with some hardware extensions. For instance, it could be beneficial to monitor some situations in which they could be hacked, unintentionally or not, by the patient.

References

1. Abdellatif, A.A., Khafagy, M.G., Mohamed, A., Chiasserini, C.: Eeg-based transceiver design with data decomposition for healthcare iot applications. IEEE Internet Things J. (2018)
2. Abdellatif, A.A., Mohamed, A., Chiasserini, C.F., Tlili, M., Erbad, A.: Edge computing for smart health: Context-aware approaches, opportunities, and challenges. IEEE Network (2019)
3. Ahmed, M., Mahmood, A.N., Islam, M.R.: A survey of anomaly detection techniques in financial domain. Future Generation Computer Systems (2016)
4. Ardito, C., Bellifemine, F., Di Noia, T., Lofù, D., Mallardi, G.: A Proposal of Case-Based Approach to Clinical Pathway Modeling Support. In: Proceedings of the IEEE Conference on Evolving and Adaptive Intelligent Systems (EAIS 2020) (2020)
5. Awad, A., Mohamed, A., Chiasserini, C., El-Fouly, T.M.: Distributed in-network processing and resource optimization over mobile-health systems. J. Netw. Comput. Appl. (2017)
6. Bhuyan, M.H., Bhattacharyya, D.K., Kalita, J.K.: Network anomaly detection: methods, systems and tools. Ieee communications surveys & tutorials (2013)
7. Cappelletti, P.: Pdta e medicina di laboratorio. La Rivista Italiana della Medicina di Laboratorio-Italian Journal of Laboratory Medicine (2017)
8. Fabius, O., van Amersfoort, J.R., Kingma, D.P.: Variational recurrent auto-encoders. In: Bengio, Y., LeCun, Y. (eds.) 3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, May 7-9, 2015, Workshop Track Proceedings (2015)
9. Haque, S.A., Rahman, M., Aziz, S.M.: Sensor anomaly detection in wireless sensor networks for healthcare. Sensors (2015)
10. Huang, Z., Lu, X., Duan, H.: Anomaly detection in clinical processes. In: AMIA Annual Symposium Proceedings (2012)
11. Leung, K., Leckie, C.: Unsupervised anomaly detection in network intrusion detection using clusters. In: Proceedings of the Twenty-eighth Australasian conference on Computer Science-Volume 38. pp. 333–342 (2005)
12. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., Elovici, Y.: N-baiot—network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervasive Computing (2018)
13. Sakurada, M., Yairi, T.: Anomaly detection using autoencoders with nonlinear dimensionality reduction. In: Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis (2014)
14. Schrijvers, G., van Hoorn, A., Huiskes, N.: The care pathway: concepts and theories: an introduction. International journal of integrated care (2012)
15. Shaadan, N., Jemain, A.A., Latif, M.T., Deni, S.M.: Anomaly detection and assessment of pm10 functional data at several locations in the klang valley, malaysia. Atmospheric Pollution Research (2015)
16. Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., Sabella, D.: On multi-access edge computing: A survey of the emerging 5g network edge cloud architecture and orchestration. IEEE Communications Surveys & Tutorials (2017)
17. Wong, W.K., Moore, A.W., Cooper, G.F., Wagner, M.M.: Bayesian network anomaly pattern detection for disease outbreaks. In: Proceedings of the 20th International Conference on Machine Learning (ICML-03). pp. 808–815 (2003)