Exploration of Data from Smart Bands in the Cloud and on the Edge – the Impact on the Data Storage Space*

Mateusz Gołosz[1 [0000−0003−1528−0431]] and Dariusz Mrozek[1 [0000−0001−6764−6656]]

Institute of Informatics, Silesian University of Technology
ul. Akademicka 16, 44-100 Gliwice, Poland
mateusz.golosz@polsl.pl, dariusz.mrozek@polsl.pl

Abstract. Wearable devices used for tracking people's health state usually transmit their data to a remote monitoring data center that can be located in the Cloud due to large storage capacities. However, the growing number of smart bands, fitness trackers, and other IoT devices used for health state monitoring pose pressure on the data centers and may raise the Big Data challenge and cause network congestion. This paper focuses on the consumption of the storage space while monitoring peoples health state and detecting possibly dangerous situations in the Cloud and on the Edge. We investigate the storage space consumption in three scenarios, including (1) transmission of all data regardless of the health state and any danger, (2) data transmission after the change in person's activity, and (3) data transmission on the detection of a health-threatening situation. Results of our experiments show that the last two scenarios can bring significant savings in the consumed storage space.

Keywords: Internet of Things · IoT · Data exploration · Cloud computing · Edge computing

1 Introduction

In recent years we are witnessing a dynamic development of various technologies that bring a revolution in many areas of our lives. Internet of Things (IoT), as a network of electronic devices that are able to communicate, interact, and exchange data with the other, is one of the leading technologies of today that have great potential to change the image of the current world and various processes on it. The IoT enters many areas of people's life, including the development of smart buildings, home automation, designing intelligent transportation, supporting smart manufacturing, farming, energy management, fitness tracking,

[*] This work was supported by pro-quality grant for highly scored publications or issued patents of the Rector of the Silesian University of Technology, Gliwice, Poland (grant No 02/020/RGJ19/0167), and partially, by Statutory Research funds of Institute of Informatics, Silesian University of Technology, Gliwice, Poland (grant No BK/204/RAU2/2019).

DOI: 10.1007/978-3-030-22744-9_47

and finally, monitoring our health state and detecting life-threatening situations. Smart bands, as well as fitness trackers, and smartwatches are wearable IoT devices that allow recognizing and monitoring the activities of people (e.g., walking, biking, jogging, sleeping) and some of their physiological parameters (e.g., heart rate, burned calories, and quality of sleep). Some of the devices can even measure the electrocardiography (ECG) signal. Sensor measurements are usually transmitted to another device that possesses higher compute capabilities, provides long-term storage of data, or acts as IoT gateway for sending the data to the other place (e.g., a data center). These can be smartphones, laptops, tablets, personal computers or other dedicated IoT devices. Data transmission is usually carried out with the use of a suitable, usually short-range and wireless communication protocol, like Bluetooth [3], Bluetooth Low Energy [12] (BLE), ZigBee [3, 7], ANT [3, 8, 10], Near Field Communications (NFC) [2, 9], or WiFi.

Wearable devices, such as smart bands and smartwatches, which are especially popular among young people, can be used not only for tracking the fitness of an individual person. These devices may also deliver valuable data that can be used for remote monitoring of someone's health state. They can be used to monitor older people or people after some serious health-related incidents, like a heart attack or stroke. In such scenarios, the data containing the information about the activity of the person and some parameters of the physiology are usually transmitted through the IoT gateway to the monitoring center where they are automatically analyzed in order to detect any risky situations. Detection of any danger should raise an alert and notify appropriate caregiver or relative who should react suitably to the situation. Since monitoring centers providing their services for hundreds of seniors require large storage spaces and analytical capabilities for the transmitted data, they are eagerly located in Cloud platforms. Cloud platforms provide scalable and almost unlimited resources for storing and performing various computations on the transmitted data. However, with the new applications of the IoT and the rapid growth of the number of users of IoT devices the amount of data transmitted to the Cloud increases very fast. This necessitates moving operations, like data processing (including assembling, transformation, and filtering) and data analysis (including data exploration with pre-trained machine learning models) on the Edge and partially free the Cloud from these operations. Edge computing assumes performing some of these operations on IoT devices and is an alternative to the centralized data processing and analysis performed in the Cloud. It prevents network congestion and storage space overload, and in some situations, may eliminate unnecessary latency.

In this paper, we show two alternative system architectures for monitoring the health state of older people with the Cloud-based centralized and Edge-based distributed data analysis. We investigate the impact of both architectures on (1) the speed of detection of dangers in health with the use of trained machine learning models and (2) the consumed Cloud storage space. We also propose alternative approaches for initiating Cloud-to-Device connectivity and transmitting data to the Cloud, which allow to reduce network traffic, the number of transactions, and bring savings in the consumed storage space.

2 Related Works

Transmission of data from IoT devices and storing the data in the storage space are important areas of the Internet of Things, since IoT devices may lead to Big Data challenges. This is reflected in several scientific works focused on IoT technologies. Authors of [5] have given a general proposition of an architecture for a system that would exchange data between wearable devices and computing Cloud. However, their work has been focused mostly on the concept of actively supporting health services, diagnosis of disease in particular. Moreover, no real data gathered from the implementation of such a system has been presented. In [6], authors have proposed a solution to a problem that occurs in a different area - lack of coherency in both input and output interfaces. The implemented framework standardizes data regardless of its size, source device, format, and structure. Zhu et al. in [14] propose a model of a gateway for a sensor network, but it does not provide any details on how the given data is being processed. Instead, it presents a very general hardware implementation and a general overview of network packet construction, server architecture and overall flow of the transferred data without going further into processing the data once it has been sent. Yang et al. [11] proposed a wearable ECG monitoring system that utilizes the Cloud platform. The work covers the hardware implementation and data transportation model and investigates the risk of heart disease. In [4] Doukas and Maglogiannis show the usage of the IoT and cloud computing in pervasive healthcare, but instead of an ECG examination, they propose quite a unique implementation of its own wearable sensor system. The system is integrated into a sock and consists of multiple sensors measuring values such as heartbeat, motion, and temperature. However, none of the above works go into details when it comes to storing and processing gathered data. Chen et al. [1] also describe the process of transferring data from wearable devices to computing clouds, but with consideration for an improvement of the wearable devices themselves. The main emphasis has been put onto integrating multiple sensors which are available as separate modules into versatile smart clothing that would constantly monitor various health indicator as well as environmental parameters, such as air pollution. On the other hand, except introducing an architecture of a model being able to transfer data from IoT devices to the Cloud, Zhou et al. [13] focuses on an emerging problem with the privacy of data collected by such devices. They describe an efficient way of encrypting and anonymizing data in the process.

None of the works listed above concentrates on the amounts of data produced by wearable devices and on ways of reducing them to a minimum. One of the ways includes changing the point where most of the data are being processed, moving the processing from the cloud itself to another (Edge) device which takes a part in the earlier stage on the data flow. In the next section, we present and compare the Edge and Cloud-based standard architectures for data processing and analysis.

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22744-9_47

3 Alternative Architectures for Monitoring Human Health State

The health and activity monitoring system for older adults with the data center located in the Cloud can adopt one of the two general architectures presented in Fig. 1. The main goal of the developed system was to determine whether a user of the wearable device (a monitored person) happened to be in a life-threatening situation. First of the presented architectures assumes classification of data and detection of dangerous situations in the Cloud. The second architecture assumes data classification on the field IoT devices (on the Edge). Both architectures consists of:

- a wearable device with sensors measuring various parameters,
- a smartphone with the Android operating system,
- a data center located in the Cloud.

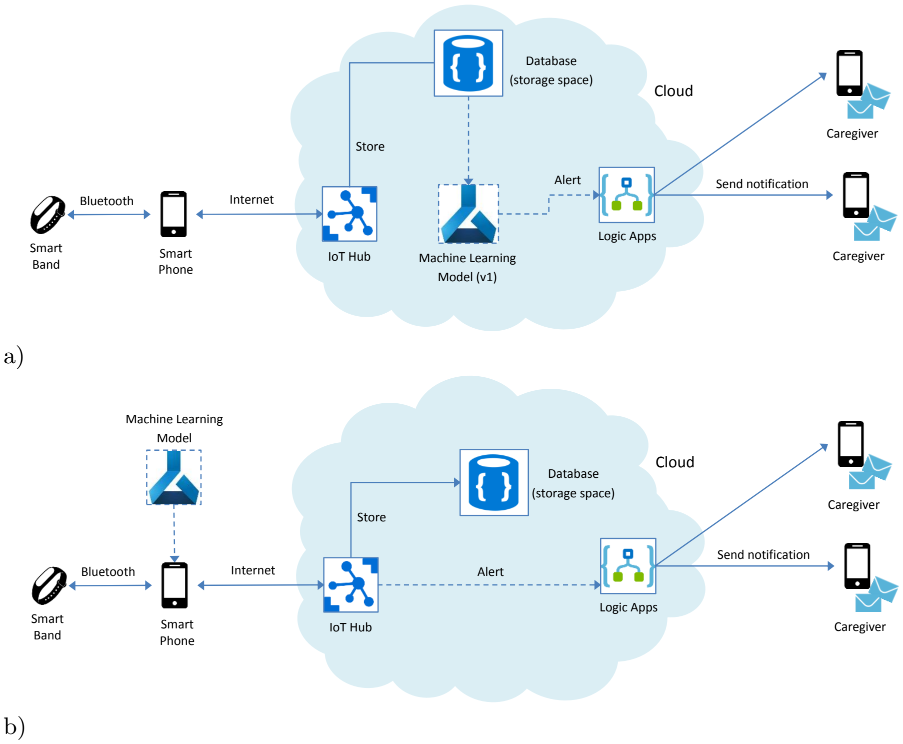

Fig. 1. Two general alternative architectures for the health state and activity monitoring system with the Machine Learning model for detection of dangerous situations implemented in the Cloud (a) and on the Edge device (b).

As the wearable device sensing various parameters of the monitored person, we decided to use the Xiaomi Mi Band 2 smart band. The smart band was selected on the basis of availability, popularity, and economic issues. One of the key points while choosing the smart band was also the possibility to access raw data from the sensors. Most smart band manufacturers do not provide the possibility to extract raw data of sensor measurements, or such a feature is limited to one extraction per 24 hours. The 24-hour period is too long for constant monitoring of the current status of a person. At the time of performed implementation of the monitoring system, there was no open-source wearable fitness tracker available on the market that would provide application programming interfaces (APIs) to extract raw data. We extracted the sensor measurements from the Xiaomi Mi Band 2 in a reverse engineering process because there was no officially supported method of gathering raw data from the smart band.

We were able to extract the following sensor measurements from the Xiaomi Mi Band 2 device:

- the number of steps made,
- heart rate,
- the quality of sleep,
- the activity currently performed, identified on the basis of the steps taken,
- the time of measurement.

For the extraction of data, we used the Gadgetbridge application for Android-based smartphones. The Gadgetbridge application is open-source software available on the GitHub platform. Apart from the Xiaomi Mi Band 2, it supports several different devices, however, we haven't tested them in our solution. The Gadgetbridge application was installed on the smartphone, which served as the IoT gateway mediating data transfers to the monitoring data center.

The remote monitoring center with a huge storage space was established in the Microsoft Azure cloud. Microsoft Azure provides scalable storage and computing resources. It offers a wide range of tools, programming languages and different platforms that can be used to develop the IoT solutions. The Cloud was also selected due to its high data security standards, global access to data with guaranteed bandwidth, and relatively easy and intuitive user interface. The Azure cloud was used to gather data transmitted from the IoT gateways (smartphones) and to store the data in the database storage repository. We tested two storage repositories in our system: Azure SQL Database – a relational database, and Cosmos DB – a document store. Data classification and detection of possible dangers on the basis of raw sensor readings were possible with the use of trained Machine Learning (ML) models. For this purpose, we used the Machine Learning Studio - an Azure module that allows for creation, training, testing, and manipulation of ML models.

The process of detection of dangerous situations in monitored persons involves a binary classification. The output of the process indicates that the person is safe or that there might be something wrong with the person. We tested multiple machine learning algorithms, like logistic regression, decision trees, support-vector machine to this purpose, but since all of them produce the same binary output and all of the trained models use the same input data for classification, changing the ML algorithm did not affect the taken storage space in any way. Therefore, this work will not focus on describing certain algorithms and models used. However, the place where the data classification occurs – in the Cloud or on the Edge – may significantly influence the network traffic and the number of data sent to the Cloud. The first approach (Fig. 1a) assumes that all data processing is done in the monitoring center, thus, all the data used for training and using the ML model are sent directly to the Cloud. The second approach (Fig. 1b) reduces the amount of data that needs to be sent by performing classification of the raw sensor readings on the Edge device before they are sent to the Cloud. Simplified data flow for both architectures can bee seen in Fig. 2.

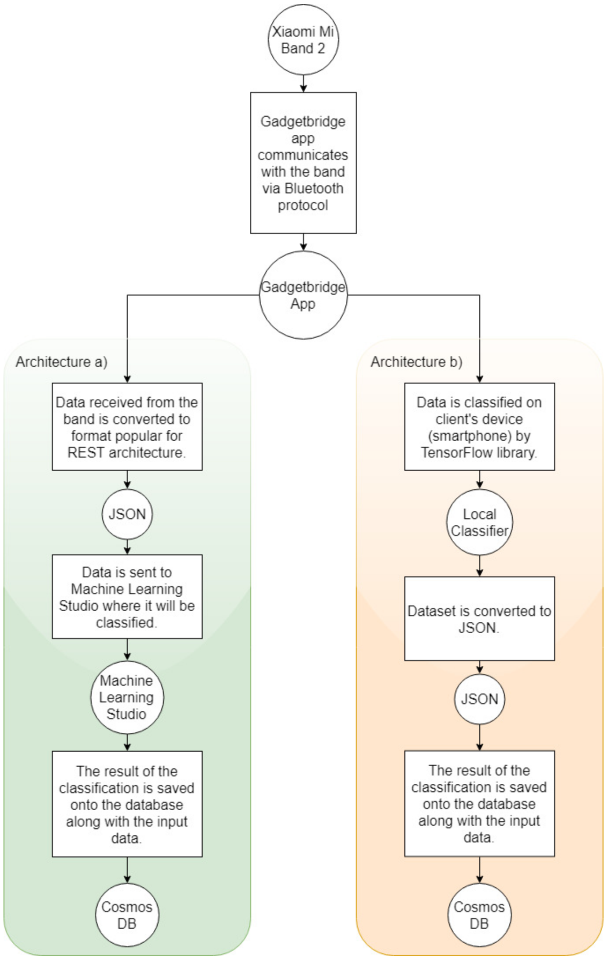
Xiaomi Mi Band 2
Gadgetbridge app communicates with the band via Bluetooth protocol
Gadgetbridge App
Architecture a)
Data received from the band is converted to format popular for REST architecture.
JSON
Data is sent to Machine Learning Studio where it will be classified.
Machine Learning Studio
The result of the classification is saved onto the database along with the input data.
Cosmos DB
Architecture b)
Data is classified on client's device (smartphone) by TensorFlow library.
Local Classifier
Dataset is converted to JSON.
JSON
The result of the classification is saved onto the database along with the input data.
Cosmos DB

Fig. 2. Data flow from the wearable device to the database.

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22744-9_47

4 The Impact of the Architecture on the Detection Speed

Both architectures presented in Fig. 1 enable detection of possibly dangerous situations in health of monitored persons through data classification, which, depending on the adopted approach, can be done in the monitoring center located in the Cloud (Fig. 1a) or on the Edge devices (Fig.1b). The classification model accepts sensor readings as the input data set. Each such a reading from the sensors located in the smart band posses the following attributes:

- Timestamp – a moment in time when the data reading occurred (a 10-digits integer),
- DeviceId – a unique identifier of the device connected to the Cloud;
- UserId – a unique identifier of a monitored person (user of the smart band),
- Raw intensity – an integer expressing the intensity of the performed activity, its values range between 0 and 99,
- Steps – an integer showing the number of steps per unit of time, which the monitored person made,
- Raw kind – a value describing the recognized activity performed by the user of the smart band (particular activities are represented as integers from the range of 0 and 99),
- Heart rate – a heart rate measured by the pulse sensor in the smart band.

The construction of the classifier that is used in the Cloud is presented in Fig. 3. The classifier is based on the pre-trained Decision Tree ML model and is available through Web service located in the Azure cloud. After the classification process the data set is supplemented by an additional attribute, called *healthy*. The attribute holds a binary value of 1 (reflecting the person is healthy) or 0 (reflecting possible health danger). Classification results are used to notify caregivers in case of dangers (through Web service output) and are saved in the database (through Export Data).

We prepared a simple benchmark to examine whether using local classifiers leads to significant impact on the detection speed. For this purpose, we measured the time between the moment when data acquisition began and the moment when the results of the classification were delivered to the client's IoT device. However, these results may vary depending on factors such as network bandwidth, data center load, CPU used in smartphone, therefore, presented values might distinctly differ in a scenario in which more users send data to the server at the same time or their mobile devices have more computing power. The results of the benchmark test performed for a single device connected to the Cloud (we used Motorola Moto X, 2014) are presented in Table 1.

5 The Impact of the Architecture on the Storage Space

There are various possibilities to store data from IoT devices in the Azure cloud, including BLOB storage spaces, relational databases, NoSQL databases, and file systems. Due to a partially structured nature of the produced data, we tested

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22744-9_47

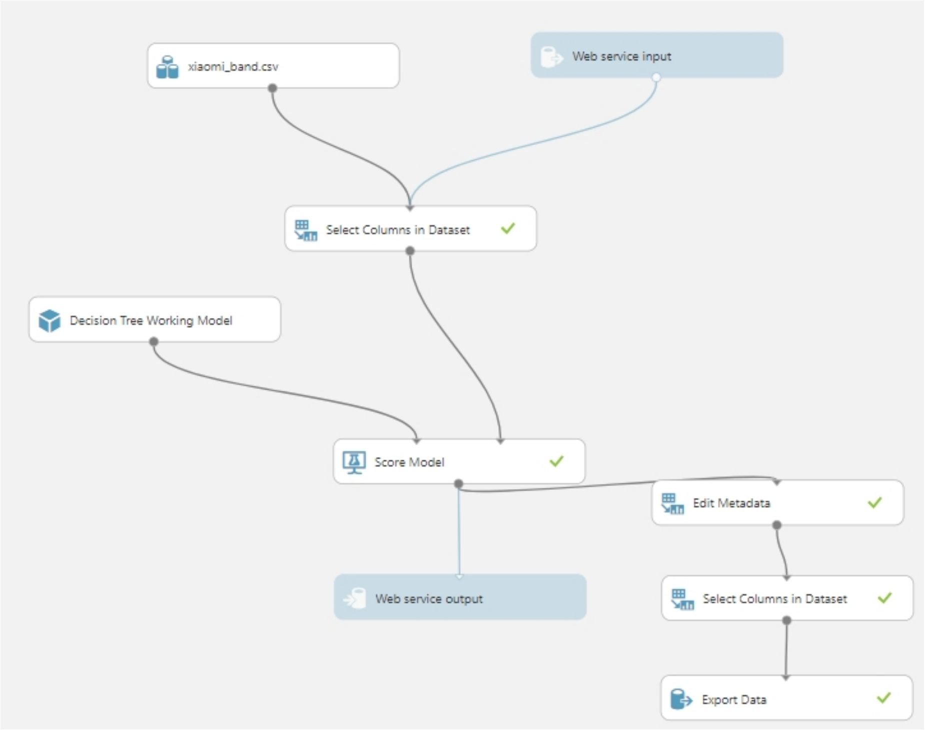

Fig. 3. Construction of the ML model providing Web service for data classification in the Cloud.

Table 1. Comparison between performance (detection speed) of local and cloud classifiers.

ML Algorithm	Average time for Azure Cloud	Average time for local classifier
Linear regression	2.96s	4.39s
Logistic regression	3.34s	4.89s
Decision tree	3.28s	5.02s
Support Vector Machine	4.87s	6.32s
Naive Bayes	3.11s	5.10s

DOI: 10.1007/978-3-030-22744-9_47

two services that offer storage space as a service, i.e., Azure SQL Database and Cosmos DB. The Azure SQL Database is a relational SQL database. It has been selected, since it provides highly available and structured data storage space among all cloud solutions. The Cosmos DB is a globally distributed, multi-model database service that supports document, key-value, graph, and columnar data models. Since data processed in our system are sent as JSON objects uniquely characterized only by the timestamp and user identifier, CosmosDB turned out to be the best NoSQL choice among available storage options in the Azure cloud. The purchase model of the Azure SQL relational database is based on the Database Transaction Units (DTUs). As a kind of currency used by the cloud customers, DTUs determine the *compute sizes* and, thus, the performance of the database, which is reflected in the compute, storage, and IO resources used by it. In Table 2 we show three different plans (also called as *tiers*) that influence capabilities, limitations, and costs for the usage of the Azure SQL relational databases.

Table 2. Various tiers defining performance capabilities for a single Azure SQL database.

Tier	DTUs	Max. available storage (GB)	Min. cost per month (EUR)
Basic	up to 5	2	4.21
Standard	10–3 000	250	12.65
Premium	125–4 000	1 000	392.13

While testing the system, we noticed that the size of data transmitted to the database and stored in it was 0.5 kB per transaction. The storage space consumed in the relational database depends on the number of transactions performed within one minute (time periods with which the Gadgetbridge application sends data to the Cloud). The time interval between successive sensor readings is one of the factors affecting the consumption of Cloud storage resources. In order to provide near real-time monitoring of a people, incoming sensor readings are processed at once and, depending on the architecture variant, whole or part of the data are immediately sent to the Cloud to be stored. For the basic variant of the Cloud-to-Device connectivity, we assumed a time interval of 1 minute, which defines how often data from the sensors are gathered and processed. This is a default, assumed value for the basic scenario with constant data transmission for every further analysis presented throughout this section. Fig. 4 shows the growth of data observed in the database within one hour for various time periods of sending data and the various number of connected IoT devices.

As can be expected the amount of data that must be stored grows with the number of monitored persons and frequency of sending data to the database. It significantly increases when the mobile application sends data every minute. This growth translates appropriately to the increase of the minimal number of DTUs that are needed since more data must be saved within a certain period of

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22744-9_47

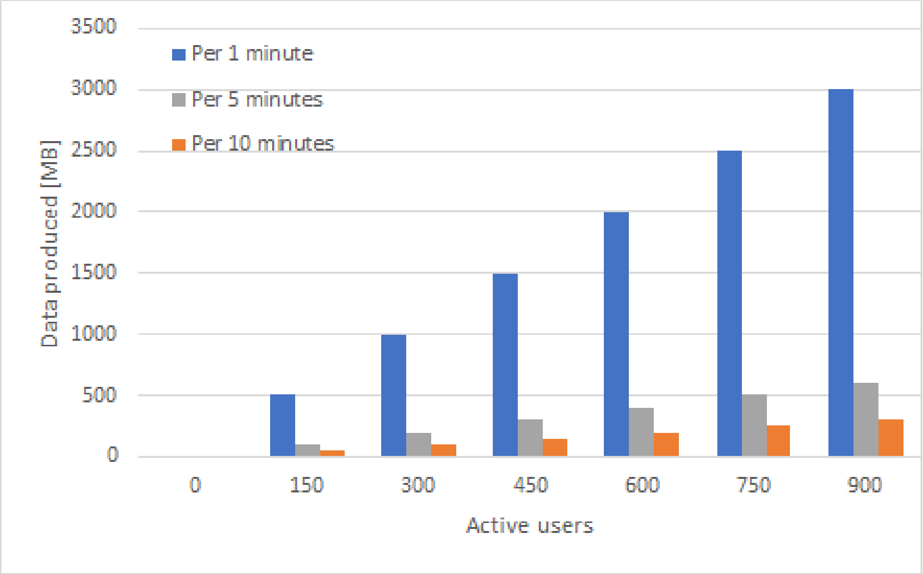

Fig. 4. The size of data produced within one hour for various time periods of successive data transmissions and the growing number of active devices and monitored persons.

time. However, more frequent data transmissions allow reacting quicker in case of detected dangers.

When using the Cosmos DB, instead of Azure SQL database, we stored data as JSON files. While testing our system, we noticed that JSON objects consume only 0.22 kB per one data transaction containing sensor readings. This is less than half of the size of the storage space taken by the same data stored in the Azure SQL relational database (0.5 kB). This difference influenced the consumption of the overall storage space and the cost. However, we cannot compare the costs directly (as sizes), since the pricing model of the Cosmos DB is not based on DTUs. The cost of usage of the Cosmos DB increases elastically with the number of transactions that are made to the database. In contrast to Azure SQL database, which makes the cost of storing data dependent of both the price of minimal number of DTUs needed for a database to operate and the storage space consumed, the cost of using the Cosmos DB is calculated differently on the basis the size of stored data, the number of requests, and the operational time. The following formula is used for this purpose (EUR):

$$Cost = g * 0.211 * req * h * 0.007, \tag{1}$$

where g is the consumed storage space (GB), req is the number of requests made per second, h is the number of hours when the database is active.

Assuming that both the relational database and the Cosmos DB perform the same number of transactions, we can compare costs of using both tested databases. In Fig. 5 we can be observe the minimum cost for both storage approaches for the various number of active users and different time periods of data transmission (1 and 5 minutes) per one hour of constant work of the particular database. As could be expected, the cost of using the Cosmos DB in the developed monitoring system is much lower than using the Azure SQL database (for the same time periods), which is even more visible for the increasing number of connected IoT devices.

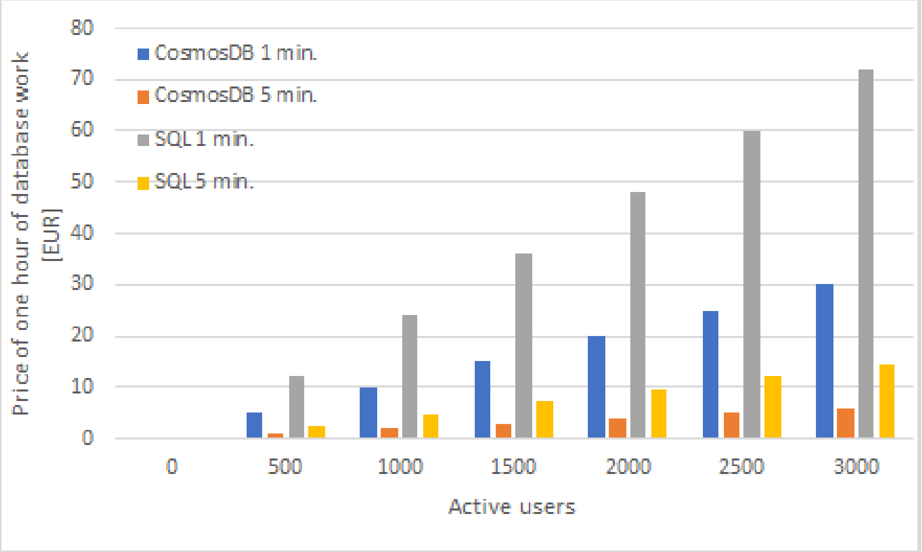

Fig. 5. Costs of using Azure SQL database and Cosmos DB (per one hour) for the various number of active users (IoT devices) and various time periods of data transmission.

The cost of storing data in one of the selected databases while constantly monitoring hundreds of persons with IoT devices remains at a reasonable level. However, it is still possible to reduce the consumption of the storage space and costs in some certain circumstances by reducing the amount of data transmitted to the Cloud. For this purpose, apart from the standard approach, when data are transmitted to the monitoring center with a given frequency, we tested two other approaches that moderate the data transmission.

The first of the implemented approaches assumes that the data from the smart band are transmitted by the IoT device only when the activity performed by a monitored person changed since the last measurement. The main idea behind this solution is that the state of the person whose life can be in danger would be very likely to change, e.g., a fainting person will probably lie down, a jogging person will probably stop and calm the heart. In this approach, the possible reduction of data transmissions and storage space consumption highly depends on the individual activity of the person during the day. Additional savings can be also expected during the night hours when most of the monitored persons should sleep for several hours. We tested this solution with the classification of the health state performed in the monitoring center, but it allowed to reduce the amount of data transmitted to the Cloud through monitoring and filtering the activity on the Edge. In the second approach, we assumed that the detection of dangers in the health state is performed on the IoT device (a smartphone). If the used classifier indicates any danger in the health state, the data are sent to the Cloud.

In Fig. 6 we can observe the comparison of all three approaches – (1) with constant, periodical data transmission to the monitoring center (with the in-Cloud danger detection), (2) with data transmission on the activity change (with the in-Cloud danger detection), and (3) with data transmission on detection of life-threatening situation (with the Edge classification on the smartphone working as the field gateway). Results show that the largest savings in the storage space and reduction of the transmitted data are achieved for the third of the implemented approaches. However, data transmission when changing performed activity is also quite effective.

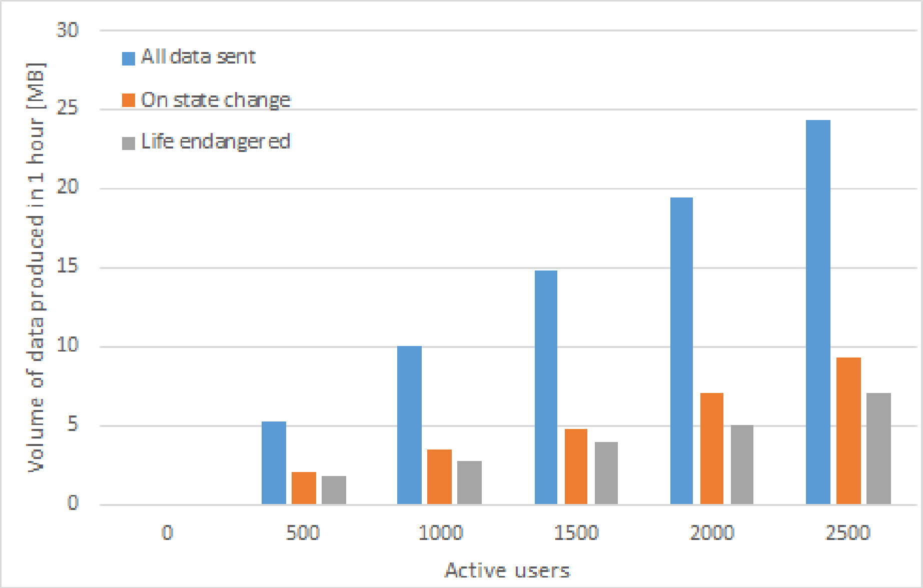

Fig. 6. Consumption of the storage space for three Device-to-Cloud connectivity approaches – constant, periodical transmission to the Cloud with detection of danger in the Cloud (All data), with data transmission only when the activity of the user changes with detection of danger in the Cloud (On state change), with data transmission only when possibly dangerous situation is detected, with detection on the Edge IoT device (Life endangered).

6 Conclusions

The growing popularity and applicability of wearable devices in monitoring people's health state leads to the increase of data that must be transmitted, stored and processed in telemonitoring data centers located in the Cloud. In consequence, this may cause network congestion and raise Big Data challenges. In this paper, we showed possible solutions of the problems by introducing event-based connectivity when the state of the person changes and by moving the burden of data processing and analysis to the Edge. Although, this may slightly decrease the speed of performed data analysis, savings in the storage space and reduction of the network traffic can be significant. Capabilities of Edge devices are also important here, since they influence, e.g., the speed of performed classification. Therefore, development of such systems may involve assembling users into a few profiled groups and apply the most cost-effective strategy to each of the group.

The results of our experiments proved that data filtering or detection of dangerous situations on the Edge device can be an effective solution not only for reducing the amount of data to be stored but also for reducing the number of transactions. Since providing a sufficient number of concurrent transactions is multiple times more expensive than storage space itself, this seems to be a proper approach. This conclusion is based on the fact that the cost of resources needed to establish a connection grows significantly faster than the cost of resources needed to save and store gathered data. This is also important for building such systems in public cloud platforms in the future.

References

1. Chen, M., Ma, Y., Li, Y., Wu, D., Zhang, Y., Youn, C.H.: Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems. IEEE Communications Magazine **55**(1), 54–61 (jan 2017). https://doi.org/10.1109/mcom.2017.1600410cm, https://doi.org/10.1109/mcom.2017.1600410cm
2. Coskun, V., Ozdenizci, B., Ok, K.: A survey on Near Field Communication (NFC) technology. Wireless Personal Communications **71**(3), 2259–2294 (Aug 2013). https://doi.org/10.1007/s11277-012-0935-5, https://doi.org/10.1007/s11277-012-0935-5
3. Dementyev, A., Hodges, S., Taylor, S., Smith, J.: Power consumption analysis of Bluetooth Low Energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario. In: 2013 IEEE International Wireless Symposium (IWS). pp. 1–4 (April 2013). https://doi.org/10.1109/IEEE-IWS.2013.6616827
4. Doukas, C., Maglogiannis, I.: Bringing IoT and cloud computing towards pervasive healthcare. In: 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. IEEE (jul 2012). https://doi.org/10.1109/imis.2012.26, https://doi.org/10.1109/imis.2012.26
5. Hassanalieragh, M., Page, A., Soyata, T., Sharma, G., Aktas, M., Mateos, G., Kantarci, B., Andreescu, S.: Health monitoring and management using internet-of-things (IoT) sensing with cloud-based processing:

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22744-9_47

Opportunities and challenges (jun 2015). https://doi.org/10.1109/scc.2015.47, https://doi.org/10.1109/scc.2015.47

6. Jiang, L., Xu, L.D., Cai, H., Jiang, Z., Bu, F., Xu, B.: An IoT-oriented data storage framework in cloud computing platform. IEEE Transactions on Industrial Informatics **10**(2), 1443–1451 (may 2014). https://doi.org/10.1109/tii.2014.2306384, https://doi.org/10.1109/tii.2014.2306384
7. Malhi, K., Mukhopadhyay, S.C., Schnepper, J., Haefke, M., Ewald, H.: A ZigBee-based wearable physiological parameters monitoring system. IEEE Sensors Journal **12**(3), 423–430 (March 2012). https://doi.org/10.1109/JSEN.2010.2091719
8. Mehmood, N.Q., Culmone, R.: An ANT+ protocol based health care system. In: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops. pp. 193–198 (March 2015). https://doi.org/10.1109/WAINA.2015.45
9. Pang, Z., Zheng, L., Tian, J., Kao-Walter, S., Dubrova, E., Chen, Q.: Design of a terminal solution for integration of in-home health care devices and services towards the internet-of-things. Enterprise Information Systems **9**(1), 86–116 (2015). https://doi.org/10.1080/17517575.2013.776118, https://doi.org/10.1080/17517575.2013.776118
10. Valchinov, E., Antoniou, A., Rotas, K., Pallikarakis, N.: Wearable ECG system for health and sports monitoring. In: 2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH). pp. 63–66 (Nov 2014). https://doi.org/10.1109/MOBIHEALTH.2014.7015910
11. Yang, Z., Zhou, Q., Lei, L., Zheng, K., Xiang, W.: An IoT-cloud based wearable ECG monitoring system for smart healthcare. Journal of Medical Systems **40**(12) (oct 2016). https://doi.org/10.1007/s10916-016-0644-9, https://doi.org/10.1007/s10916-016-0644-9
12. Zhang, T., Lu, J., Hu, F., Hao, Q.: Bluetooth low energy for wearable sensor-based healthcare systems. In: 2014 IEEE Healthcare Innovation Conference (HIC). pp. 251–254 (Oct 2014). https://doi.org/10.1109/HIC.2014.7038922
13. Zhou, J., Cao, Z., Dong, X., Lin, X.: Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions. IEEE Wireless Communications **22**(2), 136–144 (apr 2015). https://doi.org/10.1109/mwc.2015.7096296, https://doi.org/10.1109/mwc.2015.7096296
14. Zhu, Q., Wang, R., Chen, Q., Liu, Y., Qin, W.: IOT gateway: Bridging-Wireless sensor networks into internet of things. In: 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. IEEE (dec 2010). https://doi.org/10.1109/euc.2010.58, https://doi.org/10.1109/euc.2010.58