Romanian Journal of Petroleum & Gas Technology
VOL. IV (LXXV) • No. 1/2023

SECURING DATA AND APPLICATIONS IN CLOUD. CASE STUDY

Otilia Cangea

Petroleum-Gas University of Ploiesti, Romania
email: ocangea@upg-ploiesti.ro

DOI: 10.51865/JPGT.2023.01.23

ABSTRACT

Security is a principal concern when entrusting an organization’s critical information to geographically dispersed cloud platforms. In addition to the conventional IT system security procedures, designing security into cloud during the software development life cycle can greatly reduce the cloud attack surface. The paper focuses on presenting IBM Cloud security policies and their architecture and conducts a study of the security implementation steps, beginning with user's authentication on the Cloud platform. Hereinafter, the developed experimental application - a monitoring environment system - retrieves temperature, humidity, and pressure values from dedicated sensors, thus using the facilities offered by IBM Cloud platform.

Keywords: data security, environment monitoring, Cloud platform.

INTRODUCTION

Cloud technology is growing, being a new field that has many advantages for companies that choose to use it, such as cost savings, accessibility from any location, lack of investment resources, fast and secure services. There are, certainly, important risks, including data attacks, but without this technology, besides financial disadvantages, there are more hazards such as the lack of backup solutions. Thus, one may choose an implementation model according its own needs, whether it is an user or a business [1-11].

IBM® Watson™ IoT platform is a Cloud offer that allows the connection and control of sensors, home appliances, and IoT devices; thus, an user can collect data provided by the connected devices and analyze these data within its own organization [3, 12, 13].

IBM Bluemix is a Platform-as-a-Service (PaaS) environment for Cloud systems that uses Node-RED programming tool to connect objects (hardware devices, application programming interfaces – API, and on line services). The ISO standard industrial protocol used is MQTT (Message Queuing Telemetry Transport), specific to lightweight encryption, based on TCP protocol for data transmission.

An example of using IBM® Watson™ IoT platform for showing how devices communicate is displayed in figure 1 [3]. Thus, Bluemix allows the selection of sensor data types on devices and creation of dedicated applications; measured values provided by the sensors are transmitted to IBM Watson IoT platform by using MQTT protocol that offers security to data transmission. Node-RED is used for connecting these applications based on IoT services. Moreover, all these devices can be connected to the Internet and to the IBM Watson IoT Platform using an Ethernet connection or Wi-Fi.

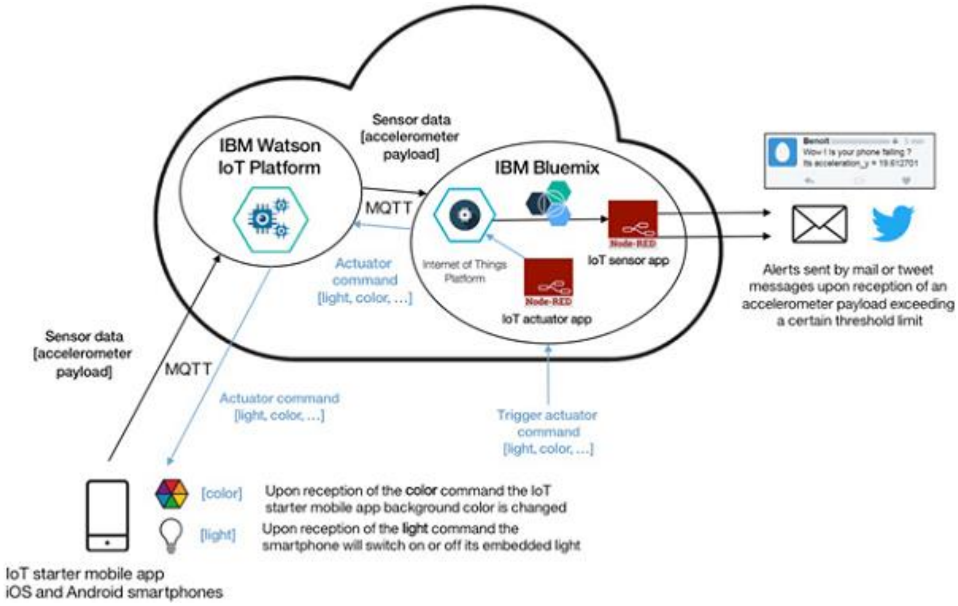

Fig. 1. *Communication between devices using IBM® Watson™ IoT platform over MQTT* [3]

STUDY OF THE IMPLEMENTATION STAGES FOR CLOUD SECURITY REQUIREMENTS

IBM Watson IoT platform offers IBM Cloud services as SaaS (Software as a Service) that allows collecting and analyzing relevant data related to products performance; these services can be extended by integrating Watson IoT platform on Blockchain platform or Watson IoT Platform Analytics [3, 12, 13].

The study implied performing the following stages for implementing the specific security requirements of the IBM Cloud platform:

- Activation of the Starter menu that automatically connects the following services:

  - IoT tools that include gateway and devices management, and application access;

  - IBM SDK (Software Development Kit) for Node.js based on JavaScript;

  - IBM Cloudant for IBM Cloud – data base for metadata storage.

- Installation of the Node-RED – based flow editor that facilitates the on-line connection of devices, APIs and services. This starting application offers a custom Node-RED version for IBM Cloud.

- During installation, user ID and password are required for securing the editor, so that only authorized users may have access.

Figure 2 presents the security levels architecture in Cloud. Node.js was used for writing the application that is implemented as a Kubernetes service Docker container with an operating system level virtualization for software development and delivery with Docker Engine software package.

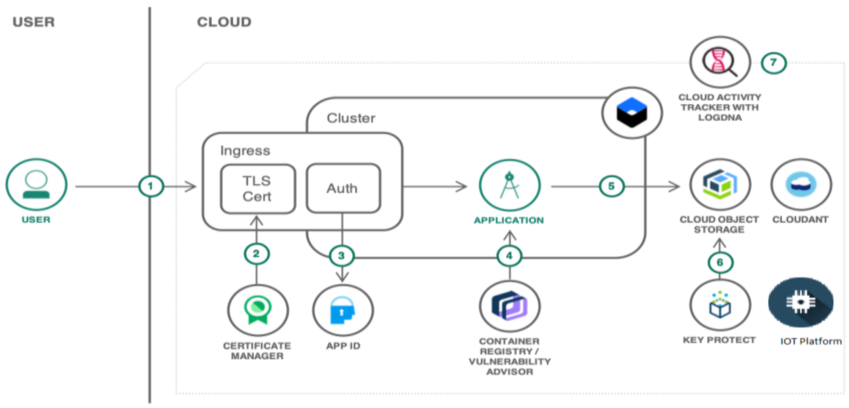

Fig. 2. *Cloud security levels architecture* [12]

Covering the levels of the structure presented in figure 2 implies the following stages:

- User connection to the application by ID and password;
- If a custom domain and TLS (Transport Layer Security) certificate are used, then the certificate is managed and implemented by a dedicated Manager;
- ID secures the application previously installed; there are applications that are automatically secured after user TLS authentication;
- The application runs in a Kubernetes cluster in IBM Registry Container Cloud. NodeJs from Container Registry is the 3rd level of security.
- The loaded files are stored in an object deposit, with specific metadata in IBM Cloudant (figure 3).
- To store the files, the user provides the key for data encryption.
- All management activities of the applications are recorded on IBM Cloud Activity Tracker.

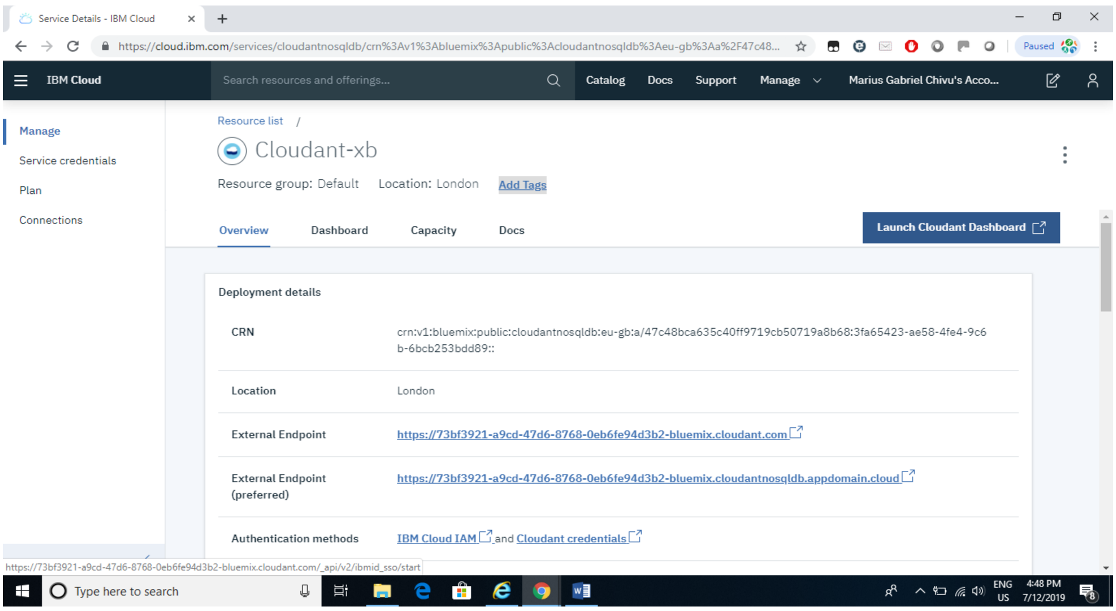

Fig. 3. *Cloudant data base generating*

MONITORING ENVIRONMENT EXPERIMENTAL APPLICATION

The developed monitoring environment application aims to acquire the values of temperature, pressure and humidity using specific sensors and transmitting the received data using MQTT dedicated protocol to a Raspberry Pi device and to the cloud. The experimental scheme is presented in figure 4.

Fig. 4. *Experimental scheme of the monitoring application: 1-Laptop; 2-Server equipped with Linux operating system; 3-RaspberryPi 3 sensors; 4-RaspberryPi 2 data bus; 5-Router.*

After performing all the connecting and configuring stages, one has to access Node-RED on Raspberry Pi 3, as presented in figure 5, where one can observe three channels, hereinafter detailed.

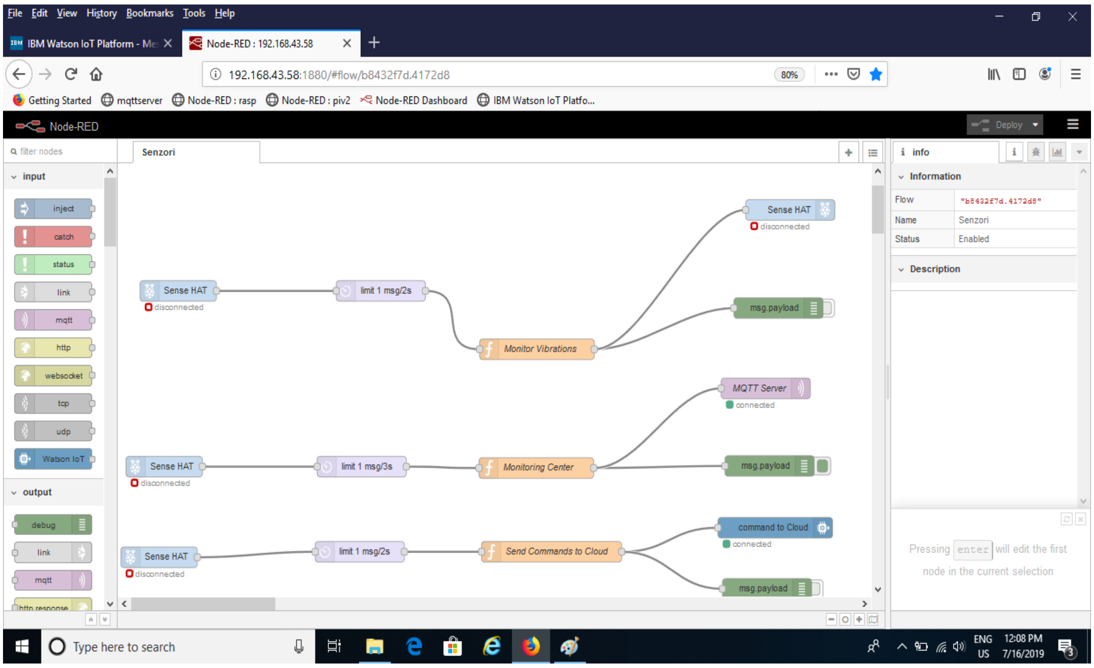

Fig. 5. *Connection to Node-RED Pi 3*

a). The first channel signalizes the presence of disturbances using the *Monitor Vibrations* module, if the Sense HAT module is connected (figure 6). Sense HAT offers an 8 x 8 LED matrix, motion and environment sensors, and a joystick. A click on *Monitor Vibrations* allows access to the specific function module. If the 3D coordinates exceed a 0.2 value, a red ALT message is displayed on the Pi3 screen; else, a white OK message is displayed (figure 7).

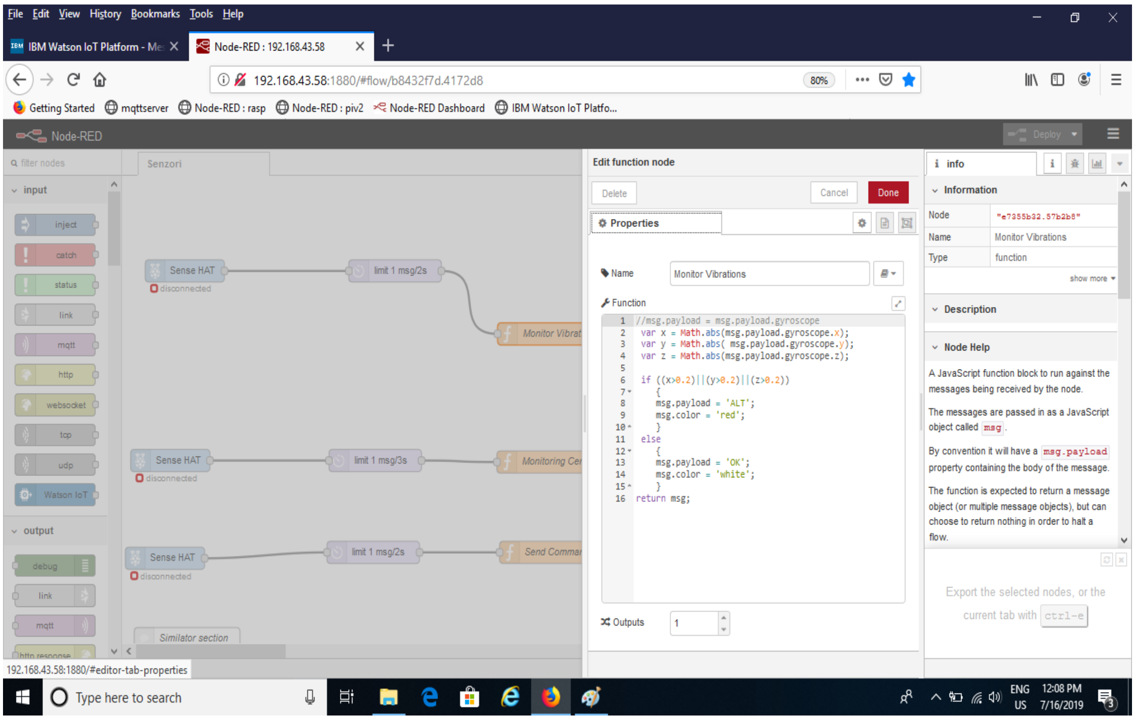

Fig. 6. *Monitor Vibrations function module*

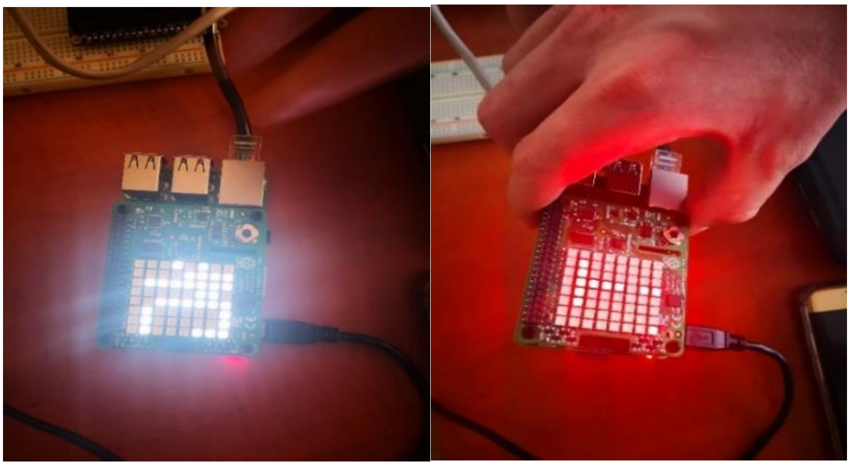

Fig.7. *Vibrations detection*

b). On the second channel, data acquired using Raspberry Pi 3 sensors and *Monitoring Center* module are transmitted to MQTT server (figure 8).

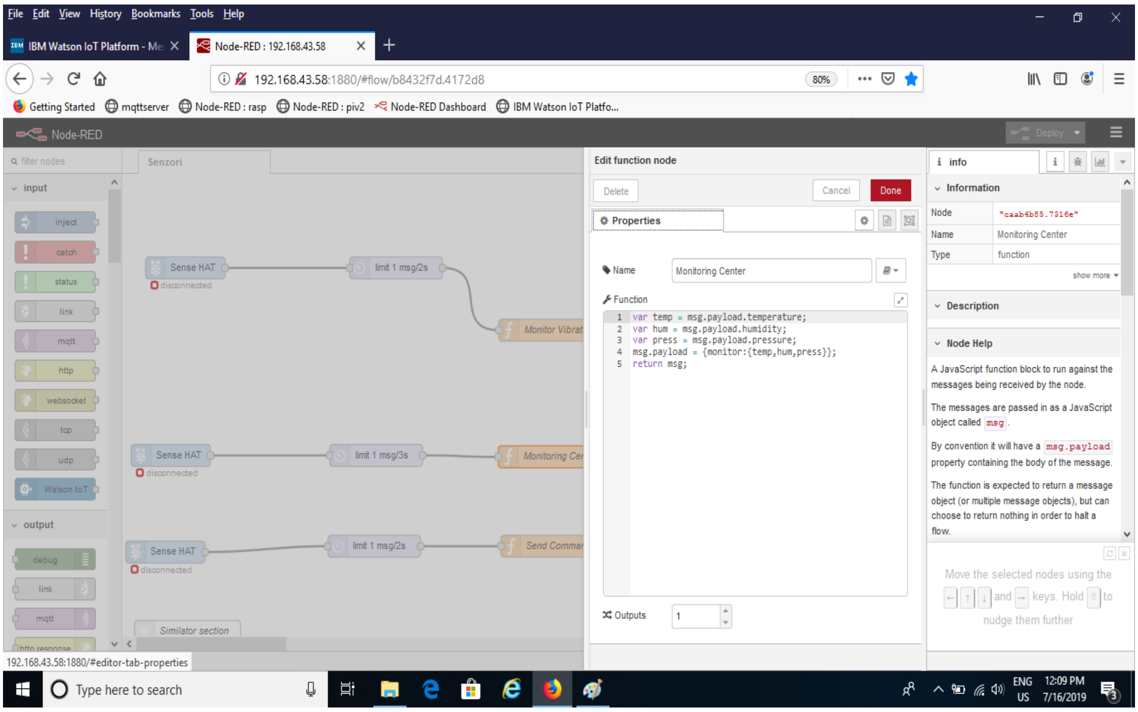

Fig. 8. Data acquisition

c). The third channel connects the server to Cloud. Using 192.168.43.147:1880 IP, one has access to Node-RED on Raspberry Pi 2, that receives data from the server (figure 9).

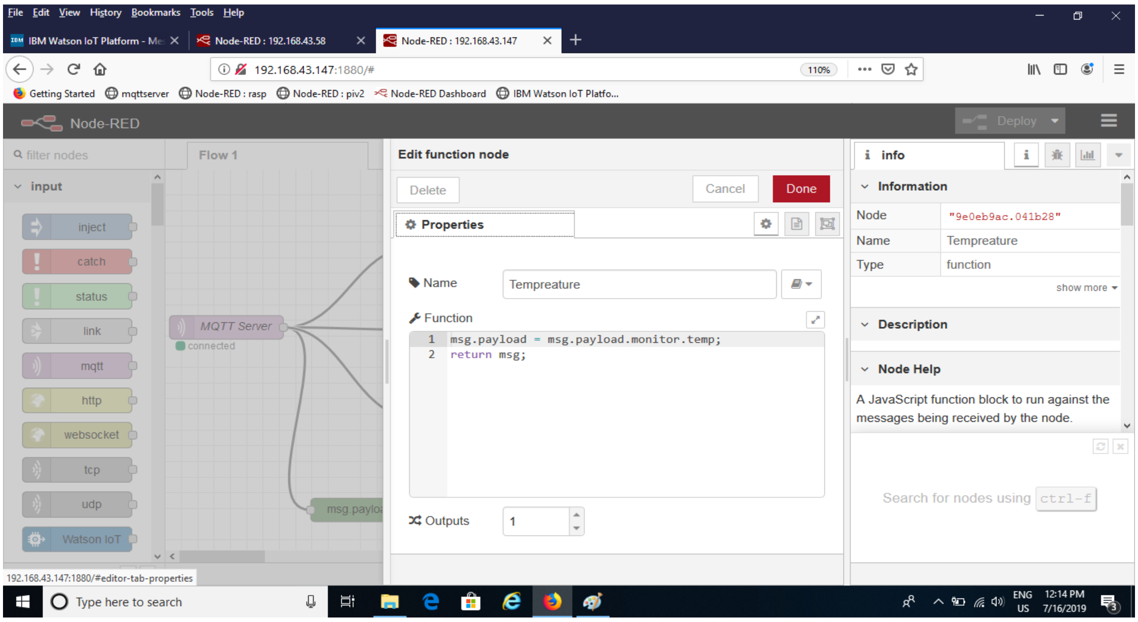

Fig. 9. Receiving data

Figure 10 presents the editing process for the graphical interface where the measured values of humidity, pressure, and temperature are displayed, as seen in figure 11.

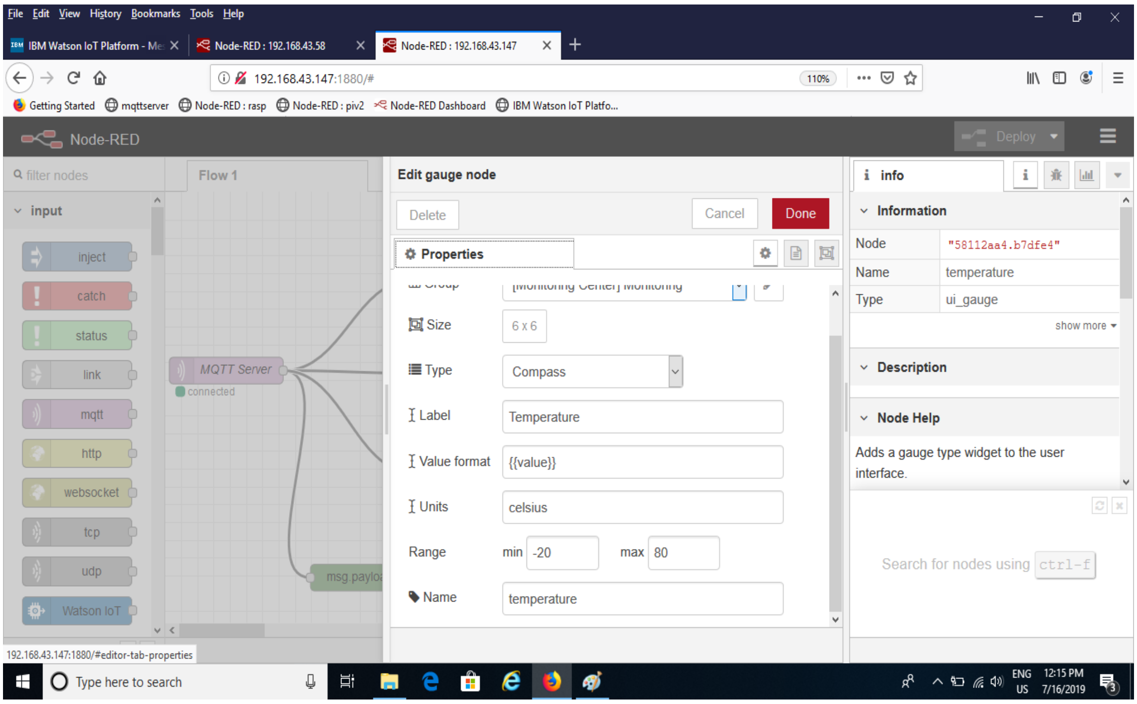

Fig. 10*. Interface editing*

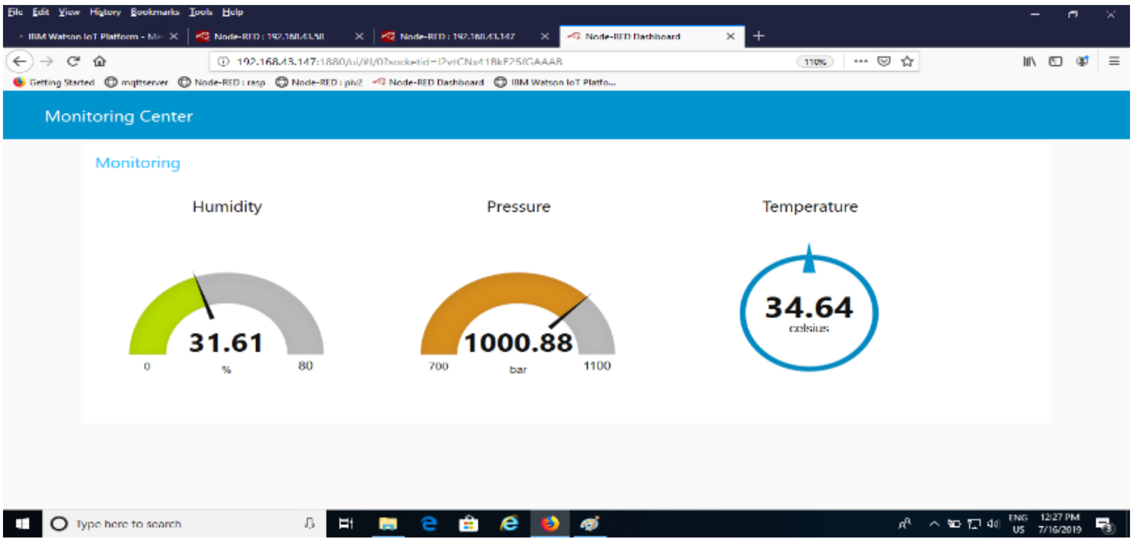

Fig. 11*. Interface display of the monitored parameters – humidity, pressure, and temperature*

To send data to Cloud, one has to access the specific connection module using Quickstart ID; thus one can perform a real-time monitoring of the data acquired by the sensors (figure 12).

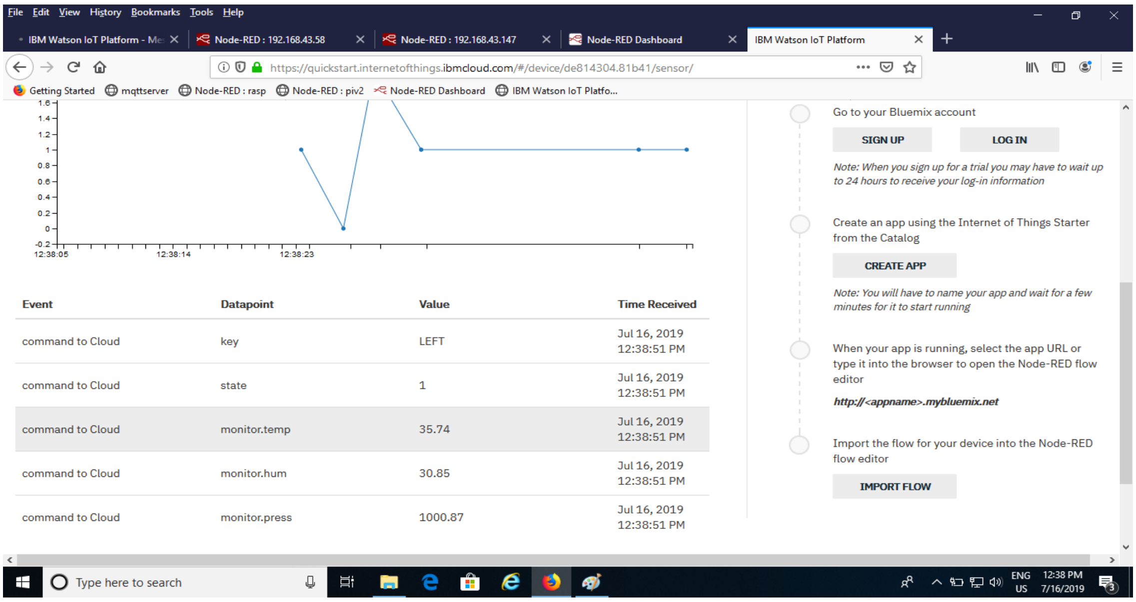

Fig. 12. *Monitoring data in Cloud*

A server monitoring is also possible using the *Monitoring* button, followed by click on *Connection*. Figure 13 presents data packages sent between Raspberry Pi 3 and the server.

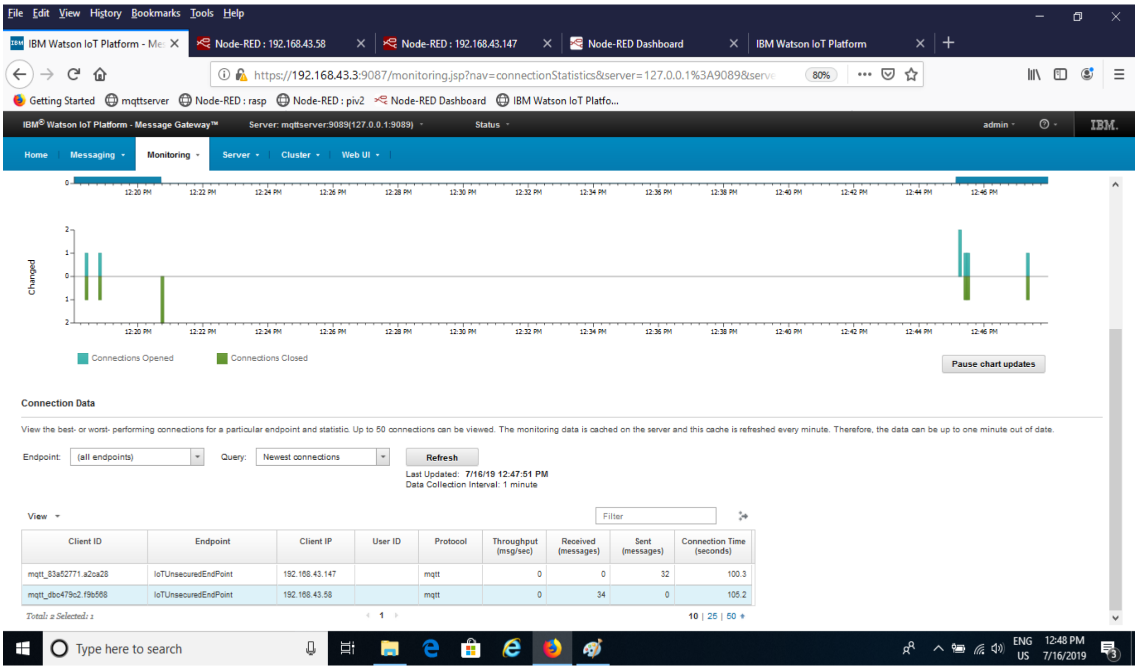

Fig. 13. *Monitoring data on server*

CONCLUSIONS

Cloud technology is in a continuous upgrade as a new field that has many advantages for companies that choose to use it, including cost savings, accessibility from any location, lack of investment resources, fast and secure services. There are, certainly, potential risks, including cyberattacks, but otherwise one can encounter more hazards such as lack of backup solutions. Cloud offers the opportunity to choose an implementation model based on the necessities of each user.

Firstly, the paper conducts a study of the required security implementation steps on IBM Cloud platform. There are three security levels, namely: the account password, the TLS certificates managed and implemented by the certificate Manager, and the Kubernetes cluster that implements the third security level, where the application is totally isolated from the exterior environment. The passwords of the applications in Cloud are stored in Cloudant and automatically encrypted.

The developed experimental monitoring system application emphasizes the features offered by the IBM Cloud platform, using Raspberry Pi 2 and Raspberry Pi 3 devices, a TP Link router, a server and a personal laptop. The aim of this experiment is to present an approach of retrieving real-time data from temperature, humidity and pressure sensors on Raspberry Pi 3, and to point how to monitor data on server and in Cloud.

Data acquisition and transmission use MQTT messaging protocol and Raspberry Pi devices interface on Node-RED that offers a browser-based stream editor that facilitates the connection of devices, API and on line services by using a large range of nodes.

The topic studied and presented in this paper is of great interest and opportunity, offering a starting point for future research directions to develop more secure complex applications that make best use of the Cloud platform resources.

REFERENCES

[1] Bhowmik, S., Cloud Computing, Cambridge University Press, 2017

[2] Gamaleldin, A.M., An Introduction to Cloud Computing Concepts, Practical Steps for Using Amazon EC2 IaaS Technology, 2013

[3] Gravelle, R., IoT Development Platforms: IBM Watson IoT Overview, October 11 2017, available at: https://www.codeguru.com/iot/iot-development-platforms-ibm-watson-iot-overview/

[4] Krutz, R.L., Vines, R.D., Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, 2010

[5] Kumar, A., Public Cloud vs Private Cloud Computing difference explained, The Windows Club, 2014, available at: https://www.thewindowsclub.com/public-cloud-vs-private-cloud

[6] Jajodia, S., Kant, K., Samarati, P., Singhal, A., Swarup, V., Wang, C., Secure Cloud Computing, Springer Science & Business Media, New York, 2014

[7] Mather, T., Kumaraswamy, S., Latif, S., Cloud Security and Privacy, O'Reilly Media Inc., 2009

[8] Rittinghouse, J.W., Ransome, J.F., Cloud Computing Implementation, Management and Security, Taylor and Francis Group, 2010

[9] Vacca, J.R., Cloud Computing Security: Foundations and Challenges, CRC Press, Taylor & Francis Group, 2017

[10] Vurukonda, N., Rao, B.T., A Study on Data Storage Security Issues in Cloud Computing, 2nd International Conference on Intelligent Computing, Communication & Convergence, India, December 2016

[11] Zbakh, M., Essaaidi, M., Manneback, P., Rong, C., Cloud Computing and Big Data: Technologies, Applications and Security, Springer Nature Switzerland AG, vol. 49, 2019

[12] *** What is the IBM Cloud platform? IBM Cloud Overview, last updated 2023-03-13, available at: https://cloud.ibm.com/docs/overview?topic=overview-whatis-platform

[13] *** Apply end-to-end security to a Cloud application, IBM Cloud tutorial, last updated 2023-02-21, available at: https://cloud.ibm.com/docs/tutorials?topic=solution-tutorials-cloud-e2e-security&cm_mmc=IBMBluemixGarageMethod-_-MethodSite-_-10-19-15%3A%3A12-31-18-_-apply-end-to-end-security-to-a-cloud-application&origin_team=TL444KVK7#apply-end-to-end-security-to-a-cloud-application

Received: May 2023; Accepted: June 2023; Published: June 2023