ECAI 2017 - International Conference – 9th Edition
Electronics, Computers and Artificial Intelligence
29 June -01 July, 2017, Targoviste, ROMÂNIA

IoT Time Critical Applications for Environmental Early Warning

George Suciu
Telecommunications Department
University POLITEHNICA of Bucharest
Bucharest, Romania
george@beia.ro

Muneeb Anwar, Alexandru Ganaside, Andrei Scheianu
R&D Department
BEIA Consult International
Bucharest, Romania

Abstract – **Catastrophes and accidents could look out for us at every moment leading to unhappy and expensive material damage or worse, to inevitable tragedies. Preventing this kind of events is a must that is taking long sessions of research, tries and development. In most cases, the cheapest and most optimized solution, which makes use of resources economically, is the one that many experts are looking for. This paper is a general overview focusing on environmental warnings, such as deforestation implying both the natural and artificial causes that stands at its basis and on analyzing and proposing some systems with both of their advantages and disadvantages. The relation of the given systems examples and the new trend of IoT (Internet of Things) is made up by cloud computing, crowdsourcing and edge computing used for filtering the most time-sensitive data from huge amount of data coming from the end devices. In addition, the paper presents some information related to climate changes and the way they affected the environment, national monitoring of these changes and the emission factor in the forests with possible solution for reducing it.**

Keywords- IoT, cloud computing, crowdsourcing, edge computing, time-critical applications.

I. INTRODUCTION

Spending time on evacuating people struck by either natural or artificial disasters could easily create panic having as result a high probability of reducing survivability. In most cases, the evacuation guidance marked with specific signs and lights such as "Exit" or "Fire exit" are inadequate and usually not taken into account by the people found in intense run for their lives. Moreover, existing emergency exit guides cannot guide people to the nearest exit leading to significant secondary casualties if the captives are guided to an exit where, for instance, a fire has occurred [1]. For the potential calamities avoidance, some disaster management methods should be implemented and somehow taught in schools. According to [2], this term represents the integration and coordination of all the activities which are necessary to build, improve and sustain the capabilities to mitigate against actual or threatened disasters. Fortunately, both population and authorities are helped by the informational technologies which present an increased involvement in disaster management, especially for fast prediction, communication and dangers awareness [3]. Nowadays sensors are used more and more, being found in almost every electronic device. WSNs (Wireless Sensor Networks) consists of sensor nodes spread in locations of interest and depending on their features, sensors can be divided into flame/smoke/heat detectors, vibration/ultrasonic/location control sensors etc.

The Internet of Things (IoT) represents a network of physical end devices such as sensors, mobile devices, PCs etc., which are further integrated within electronics, software and network connectivity in order to enable these end devices to collect, measure and exchange data between them. Over the last period, IoT gathered a lot of interest in many domains and according to the experts, it is estimated that by 2020, almost 50 billion objects will be interconnected via IoT [4]. The process of obtaining and analyzing the collected information generated by a huge number of end devices is defined as crowdsourcing. Cloud computing is a modern concept widely used for the services to handle data traffic and application implementation over the IoT. It makes computer applications, hardware and application development platforms as available services over the Internet. These services are mainly known as Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). IoT technologies are not able to stop the disasters from taking place, but it can be useful to predict them, to put in guard both authorities and population through early warning systems and to offer a fast solution in rescuing the possible victims of the catastrophes. Due to the fact that the integration of crowdsourcing IoT data with cloud computing platform has limitations caused mainly by the latency within networks, the users cannot interact with the real-time events/disasters, hence the possibility of implementing of the edge computing must be considered in order to overcome this weakness. This paradigm works like a filter so that, instead of analyzing or sending a huge amount of data, edge computing selects the most time-sensitive data, close to where it is generated [5].

In this paper, our aim is to present two use-case scenarios which were implemented to monitor

978-1-5090-6458-8/17/$31.00 ©2017 IEEE

different environmental parameters, describing all the necessary technical specifications and the used cloud computing architecture. The rest of the article is structured as follows. Related work is presented in Section II. In Section III will be described the functional description, while the conclusions and future work are provided in Section IV.

II. RELATED WORK

Sensors are becoming part of our lives little by little even if most of the people could not admit this fact or could not see the advantages of these devices. They are widely used in different domains of applicability fulfilling many tasks that we had to accomplish some years ago. WSNs incorporate spatially distributed autonomous equipment that make use of sensors to monitor specific environmental parameters. These wireless networks can be related easily with the IoT and cloud computing (and its derivatives) concepts since, according to its definition, IoT represents an inter-networking of physical devices that are embedded with electronics, sensors, software etc. As for critical applications, there have been developed many systems having as principal goal the prevention or quick intervention in a short limited period of time.

For instance, [6] proposed an energy-efficient WSN architecture for monitoring illegal logging. This was done by analyzing the existing algorithms for chain-saw detection, sound source and source node localization. In [7] the authors propose a WSN observation system for visualizing the physiological parameters of the patients in the hospital. Sensors/detectors for blood pressure, ECG, SPO2 are used in concordance with a GPS for providing the status of the patient and a microcontroller that collects the incoming data from the analog sensors, converts them into digital and send them to a web server. On the other hand, [8] came up with a WSN surveillance system for monitoring the possible burglaries. The system comprises a module for monitoring, one for detection and another one for communication. In addition to this WSN system, a surveillance management system for collecting data from all sensors, cameras and an end user system are presented.

As a WSN represents a network which has many restraints, it becomes very difficult to employ the security approaches directly to the WSN area. The security path needs secured resources for the sensors implementation, which also adds the code storage and data memory. The sensor consists of a very less amount of memory and storage space in the code distribution. The security system is made only in the condition of limited code size for the security design. Power limitation is one of the biggest impulsions to wireless sensor capabilities, where the sensor nodes are deployed in a sensor network which cannot be recovered or recharged.

Unreliable communication is another drawback in the sensor security [9]. In this case the security is totally depending on the protocol, which is supported on the communication as follows:

- Unreliable Transfer: the routing of the sensor is connectionless and therefore it is very unreliable. Overcrowding of nodes causes the packets of the sensor to be damaged and results in missing data packets;
- Conflicts: In this case the communication can still be unreliable because of the broadcasting nature of the wireless sensor network. The main reason for this conflict is the meeting of the packets in the middle of the transfer and would result in the failure of the transfer. This seems to be one of the major problem due to traffic of the sensor network [10];
- Latency: Latency takes place due to multi-hop routing. This means that the message needs to hop over several subsystems until it reaches the final destination. The integration between the sensor nodes becomes hard to be obtained. Congestion happens and retransmission should be done [11].

III. FUNCTIONAL DESCRIPTION

In this section we present the functional description of the system used for environmental early warning and two use-case scenarios that were implemented to monitor the environmental parameters.

The cloud computing architecture is divided in two parts, namely the front-end and the back-end. The connection is made by connecting to each other with the help of a network, virtual network or the Internet. The front-end is the side with machine user, and the back-end is the cloud part of the system.

A. Front-end architecture

Front-end architecture represents the side that is visible to the client, user or the customer. It builds the client's network or machine system that is used for achieving the cloud system. Not all the cloud computing systems provide an equal interface to users. In case of web programs, the support is driven from web browsers like Chrome, Firefox, and Internet Explorer.

B. Back-end architecture

Back-end is the side used by the service provider, which includes different servers, machines, data storage systems, and virtual machines that together establish the cloud computing services. This system has options of various types of computer programs, and every application in this system is constructed by its own committed server. The back end is responsible for providing security systems, traffic control and protocols. Back-end helps employ protocols that connects networked machines for communication, our approach being based on SWITCH project [12]. The components specified in SWITCH were used to develop a EWS (Early Warning System) for collecting real-time data from sensors and processing the received data for the public to have easy access to information regarding accidents and calamities.

C. Environmental early warning system

The traditional framework of an early warning system has three phases: the forecasting of potential

events, the precursors monitoring, and the alert or warning notification in case of disaster. The national agencies for emergency situations have promoted a four-step framework, which provides a fourth phase: when a warning has been noticed, the onset of the activities responsible of emergency response will take place. As it can be seen in Fig. 1, the purpose of the fourth phase is the recognition of the fact that responses to the warnings needs to take place.

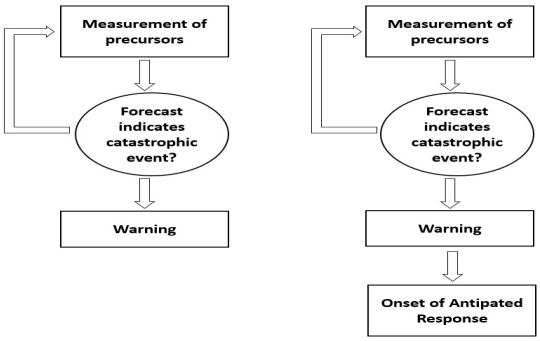

Figure 1. Early warning system phases

D. *Scenarios for monitoring the environmental parameters*

1) *Extended Region Monitoring*

Disasters like floods and earthquakes are usually followed by the need to manage in an effective way the large data amount provided by the sensors (such as information about relief personnel and victims, damages to infrastructure and buildings, weather, geographical data about the road infrastructure and weather information), to provide the possibility of giving proper responses when disasters occur.

In this case, if there is a disaster warning made by the Government, the system will take the warning into account, increase the monitoring (collecting more data, which implies increased resource usage) and notify the users.

In this scenario were used 100 sensors to transmit parameters, which are collected by the RTU and forwarded to IP Gateway using GSM/GPRS. CC Server is responsible for the reception and transmission of the parameters to the Notification Server, as shown in Fig. 2. Also, the virtual machine/container specifications are listed in Table 1.

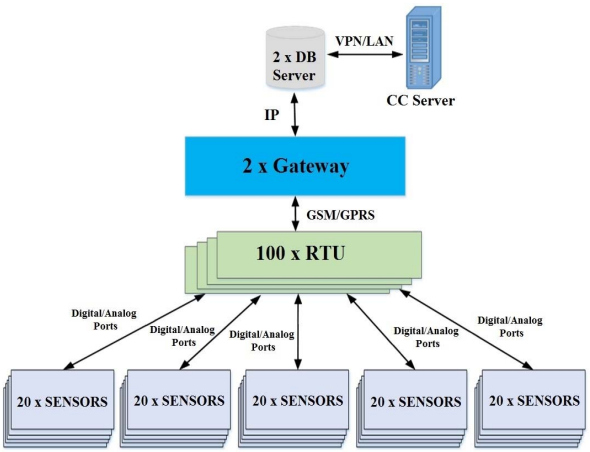

Figure 2. Extended Region Monitoring diagram

TABLE I. VIRTUAL MACHINE/CONTAINER SPECIFICATIONS SCENARIO 1

	Gigabit	CPU	RAM	HDD
DB Server	2	2.4GHz or higher, 4-core or higher	8GB	2TB
CC Server	1	2.4GHz or higher, 6-core or higher	16GB	1TB

The DataBase Server (DB) is a MySQL type database. The Call Center Server (CC) consists of an Nginx application which represents the Notification Server. In this scenario were used 100 sensors for transmitting the parameters collected by the Remote Telemetry Unit (RTU) in normal mode. Using GSM/GPRS, the parameters will be forwarded to the IP Gateway, which has the role to store in the database the received parameters. The Call Center Server is responsible for the transmission of the parameters to the Notification Server, and reception.

2) *Monitoring other environmental parameters*

The main purpose of this scenario is to identify and to record the presence of pollution in air and water by sending spatial or qualitative data (for example, GPS coordinates) about specific incidents to people and authorities who has mobile devices with Internet services available. The scenario was developed for the Black Sea and the Danube River monitoring.

In this scenario 50 sensors were used to transmit different parameters which are collected by the remote telemetry unit and forwarded to the IP Gateway using GPRS/GSM. Responsible for the reception and transmission to the Notification Server of the parameters is the CC server, as it can be seen in Fig. 3. Also, the virtual machine/container specifications are listed in Table 2.

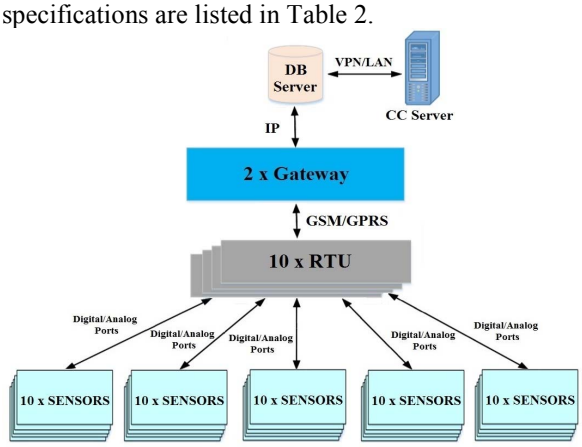

Figure 3. Monitoring other environmental parameters diagram

TABLE II. VIRTUAL MACHINE/CONTAINER SPECIFICATIONS SCENARIO 2

	Gigabit	CPU	RAM	HDD
DB Server	1	2.4GHz or higher, 4-core or higher	8GB	1TB
CC Server	1	2.4GHz or higher, 4-core or higher	8GB	1TB

The systems described in the above scenarios have been successfully implemented by BEIA Consult in specific locations on the Romanian territory and are

currently providing relevant information for detecting natural disasters (floods, etc.)

3) Adaptability of the application

In Fig. 4 is presented the way how the application should be adapted to dynamic conditions.

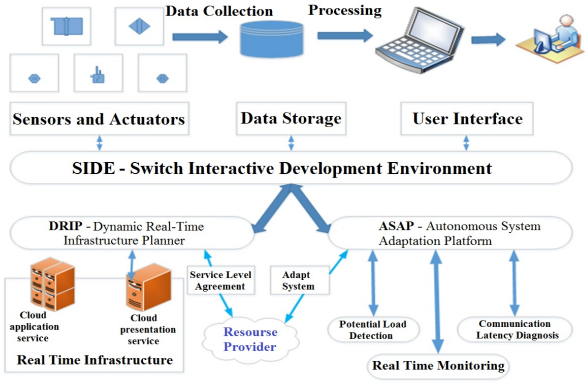

Figure 4. Adaptability models

The EWS developers will benefit of an intuitive interface which is provided by the SIDE (SWITCH interactive development environment) subsystem:

- *Describing the application logic:* facilities of the virtual call center, activation of different warning services, processing, data storage and the collection of data provided by sensors;
- *Defining the individual processes level and/or the quality requirements at system level.* SIDE provides a formal mechanism for validating the time related requirements. Also, it creates the constraints regarding the application development;
- *Selecting the potential Cloud providers and describing the quality requirements and costs for the runtime environment.* If it's necessary, users can also describe AVIs (Abstract Virtual Infrastructures).

The main function of the DRIP (Dynamic Real-time Infrastructure Planner) subsystem is to create a concrete VRI (Virtual Runtime Environment) which is based on the SIDE input, and to create a SLA (Service Level Agreement) for negotiating with providers and deploying different services to the VRI after it was provisioned.

The ASAP (Autonomous System Adaptation Platform) subsystem role is to detect the waiting time of an average customer for contacting the call center, the sensors communication latency and the potential load. Also, ASAP subsystem is responsible of tuning in a dynamically manner the application execution, by adapting the execution.

4) GIS (Geographic Information System) and WMS (Web Map Service) Interface Standard

To analyze, manage, capture and display the information on a map, a GIS software was developed especially for this kind of activities. This software allows the users to visualize, interpret, question and understand the parameters provided by different sensors, revealing patterns, relationships and trends in the form of charts, reports, globes and maps.

The WMS Interface Standard provides a HTTP interface used to request from more distributed GDBs (Geospatial Databases) geo-registered map images. The response to the request can be seen in any browser application and it consists in map images geo-registered as PNG, JPEG formats.

IV. CONCLUSIONS

The implementation of early warning system used for early warning of hazardous environmental events represents a challenging domain, because the configuration of an elastic cloud must be performed. In this paper was presented a short description of the IoT use-case scenarios implemented to monitor the environmental parameters, describing the innovative cloud computing architecture and the technical specifications necessary to fulfil different functional requirements. As future work, we envision the upgrade of existent wireless sensor network already implemented with near real-time operating systems.

ACKNOWLEDGMENT

The current research and development project has been funded by the research and innovation program of European Union's Horizon 2020 under grant agreement No 643963 (SWITCH project). The project was partially supported by UEFISCDI Romania under grant E-STAR.

REFERENCES

[1] C.S. Ryu, "IoT-based Intelligent for Fire Emergency Response Systems", International Journal of Smart Home vol. 9, no. 3, pp. 161-168, 2015.

[2] S.C. Arranz and P.M. Danalache "Non-Governmental Organizations and Communities' Protection" FAIMA Business & Management Journal, vol. 4, no. 1, pp. 5-9, 2016.

[3] B.J. Reynolds and G. Shenhar, "Crisis and Emergency Risk", Koenig and Schultz's Disaster Medicine: Comprehensive Principles and Practices, pp. 390-394, 2016.

[4] S.E. Collier "The emerging enernet: Convergence of the smart grid with the internet of things", IEEE Industry Applications Magazine, vol. 23, no. 2, pp. 12-18, 2017.

[5] A. Rauniyar, P Engelstad, B. Feng and D. V. Thanh, "Crowdsourcing-based Disaster Management using Fog Computing in Internet of Things Paradigm", In 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC), pp. 490-494, 2016.

[6] L. Petrica and G. Stefan, "Energy-Efficient WSN Architecture for Illegal Deforestation Detection", International Journal of Sensors and Sensor Networks, pp. 1-4, 2015.

[7] R. Rajeswari "A Healthcare Monitoring System Using Wireless Sensor Network With GSM", International Research Journal of Engineering and Technology (IRJET), pp. 1-4, 2017.

[8] S. Saha and S. Neogy, "A Case Study on smart Surveillance Application System using WSN and IP webcam", Applications and Innovations in Mobile Computing (AIMoC), pp. 36-41, 2014.

[9] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks." IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, 2002.

[10] J. P. Walters, Z. Liang, W. Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in distributed, grid, mobile, and pervasive computing, pp. 367-341, 2006.

[11] C. Lu, A. Saifullah, B. Li, M. Sha, H. Gonzalez, D. Gunatilaka, C. Wu, L. Nie and Y. Chen "Real-time wireless sensor-actuator networks for industrial cyber-physical systems" Proceedings of the IEEE, vol. 104, no. 5, pp. 1013-1024, 2016.

[12] Z. Zhao, P. Martin, J. Wang, A. Taal, A. Jones, I. Taylor, V. Stankovski, I.G. Vega, G. Suciu, A. Ulisses and C. de Laat C "Developing and operating time critical applications in clouds: the state of the art and the SWITCH approach" Procedia Computer Science, vol. 68, pp. 17-28, 2015.