International Conference on Automation, Control Engineering and Computer Science (ACECS)
Proceedings of Engineering and Technology – PET
Vol.21pp.47 -52

The Internet Of Things In Oil And Gas Industry: A Multi Criteria Decision Making Brokerage Strategy

Maurizio Giacobbe*, Riccardo Di Pietro†, Angelo Zaia‡ and Antonio Puliafito†
*Insirio SpA
Via Castello della Magliana, 38
00148 - Roma, Italy
Email: mgiacobbe@insirio.it
†CIAM, University of Messina
Piazza S. Pugliatti, 1
98100 - Messina, Italy
Email: {rdipietro, apuliafito}@unime.it
‡Arduino.org
Via Romano, 12
10010 - Scarmagno, Torino, Italy
Email: angelo@arduino.org

***Abstract*—The advent of the Internet of Things (IoT) is changing the way to conceive distributed systems. Nowadays, we can talk about IoT and Cloud computing to indicate a new type of distributed system consisting of a set of smart objects which are interconnected through the Internet with a remote Cloud infrastructure, platform, or software. IoT promises to achieve new benefits in several industrial businesses. Among these, the *Oil and Gas (O&G)* industries can achieve the greatest benefit by using the IoT as enabler of new sources of information. In this paper, a simulation-based *Multi Criteria Decision Making (MCDM)* brokerage strategy is presented. The goal is to allow cooperative small-medium size IoT Cloud providers to satisfy the request for IoT-Cloud services, with a good compromise between service level and business for the O&G industries.**

I. Introduction

The proliferation of a wide variety of Internet-connected and low-cost devices is leading to the development of the revolutionary communication paradigm known as the Internet of Things (IoT) [1]. It allows both public and private organizations to combine always-connected, non-invasive, smart objects (Things) [2] to improve everyday human activities.

Moreover, the combination between IoT and Cloud computing is pursuing new levels of efficiency in delivering services [3]. The emerging business perspectives coming from IoT are pushing private, public, and hybrid *Cloud Service Providers (CSPs)* to integrate their systems with embedded devices (including sensors and actuators) in order to provide new services. As a consequence: i) new types of providers have been rising that combine the traditional Cloud computing paradigm with IoT; ii) new type of distributed system have been designed. They consist of a set of smart devices interconnected with a remote Cloud infrastructure, platform, or software through the Internet, in order to provide Sensor and Actuator as a Service (SAaaS).

Furthermore, *Community Cloud* is an emerging topic. It is built and provisioned by its members and it can be owned and managed by the Community itself, by a third party, or a combination of both. A small or medium size CSP which receives IoT service requests from customers and is unable to satisfy whole requests by allocating suitable and affordable resources at its data-centers, can take part in a "community" [4]. The resulting benefits, costs (i.e., money) and responsibilities are shared among the Community CSPs. These latter will be able to offer IoT-Cloud services through private data-centers, i.e. by *private Clouds*, they can be commercially offered for customers, i.e. by *public Clouds*, or yet it is possible that both public and private Clouds are combined forming *hybrid Clouds*.

In any case, the IoT-Cloud union can demand a wide range of new "big data" capable technologies and services in order to manage both semi-structured and unstructured data. About this "big data problem" the total amount of data created (and not necessarily stored) by any device will reach 600 ZB per year by 2020 [5].

In such scenario, the IoT-Cloud union is creating a new digital agenda for Oil and Gas (O&G), thus changing the way to conceive distributed systems to serve this business.

To be leader an O&G company needs to innovate its industrial control systems by using IoT as a new model to integrate information from data gathered, employees and industrial processes across its supply chain. This progress can result in new business opportunities, especially in to keep human safety in the industrial plant. Studying IoT innovation and the early

ISSN 2356-5608

use cases will help Chief Information Officers (CIOs) and IT leaders towards a strategic perspective to capture business value from the IoT-Cloud union.

Insirio SpA pays serious attention to the above-mentioned necessities. It develops Information Technology solutions for the Owner Operators, the *Engineering Procurement Construction (EPC)* Companies and their suppliers and sub-contractors. Its experience in a hundred projects for the O&G industry addressed the presented work to understanding the feasibility of the IoT application in O&G. In this regard, the use of IoT in O&G Industry is feasible in the construction site phase (e.g., traceability of specific modules for pipelines, human safety devices), and not in the executive and maintenance phases. The reason is due to the current know-how and the difficulties in using "open" hardware and software (e.g., *Arduino*) by suitable low-cost smart objects for executive and maintenance, in compliance with safety conditions.

II. Motivations

O&G companies can control their processes by using smart objects and deployed services capable to act locally on the data they generate, while still using the Cloud for data management, analytics, and durable storage.

Such scenario demands timely, repeatable, and controllable methodologies for evaluation of algorithms, applications and policies before the development of IoT-Cloud services, especially to achieve a good compromise between several *heterogeneous* indicators. Generally, real testbeds would seem the best choice. However, since the use of real testbeds limits the experiments to the scale of the testbed, thus making the reiteration of results an extremely difficult undertaking, alternative approaches need to be considered. Among these possible alternatives, **simulations tools** allow researchers and practitioners to evaluate working hypothesis before the software development. The above approach is fundamental for IoT-Cloud environments, because access the infrastructure incurs payments in real currency (*pay-as-you-go* system). Simulation tools can offer significant benefits both for customers and CSPs.

1) Customer-side Benefits: Customers can test their IoT and Cloud services in repeatable and controllable environment, without additional cost. Moreover, a customer can evaluate the amount of smart objects to use and raw data to transmit to the Cloud in order to contemporary reduce costs and to increase the quality of the data.

2) CSP-side Benefits: At the CSP-side simulators can allow evaluation of different scenarios where to allocate IoT-Cloud resources under varying performances, workload conditions, and monetary cost distributions. A Community CSP can proceed in its *business analysis* thus to optimize the resource access cost with a special focus on improving profits.

In the absence of such simulation-based environments, both IoT-Cloud customers and CSPs risk to commit serious errors of assessment, or to refer to non-objective evaluations, resulting in inefficient service performance and economic losses. Therefore, both for customers and CSPs, simulations-based environments allow to evaluate the hypothesis prior to the software development, thus reducing the risk of economic losses and scarce *Quality of Service*. In such a context, to provide CIOs and IT leaders with guidelines for managing their digital transformation investment objectives and implementation strategies is a priority.

For the above reason, in this paper a simulation-based *Multi Criteria Decision Making (MCDM)* brokerage strategy is presented. The goal is to allow cooperative small-medium size IoT Cloud providers to satisfy the request for IoT-Cloud services, with a good compromise between service level and business for the O&G industries.

III. Related Work

In this Section we present related work concerning the use of IoT in Industry and the massive sensing data management through the Cloud according to the industrial necessities.

In the past, *Wireless Sensor Networks (WSN)* was not the preferred choice for offshore monitoring in the O&G sector for many reasons, such as reliability and security concern. Nowadays, instead, advances in reliability, security, and affordability within the constraints of frequency allocation enable O&G companies to take full advantage of WSN for challenging industrial environments. About this topic, an industrial pipe rack safety monitoring system based on WSN, which uses the ISA100.11a standard for industrial field instruments is presented in [6].

Standardization efforts on IoT and machine-to-machine communication are addressing *industrial-strength networking* in multiple forums: a viewpoint about *Intelligent Systems* as a new industrial revolution is described in [7].

In [8] the authors address at massive sensing data management in the Cloud. It includes a framework supporting parallel storage and processing of massive sensor data in Cloud manufacturing systems, based on Hadoop MapReduce.

A context-oriented data acquisition and integration platform for the IoT over a Cloud is presented in [9]. The platform collects sensor data from different types of sensor devices and integrates them into semantic contexts which can be easily shared and reused among different mobile applications. As a consequence, the context information can enhance mobile applications usability by adapting to conditions that directly affect their operations.

In [10] the authors propose a *Sensor-Cloud Infrastructure* which can manage physical sensors on IT infrastructure to improve the usability through virtual sensors on Cloud computing. The Missouri S&T (Science and Technology) sensor Cloud [11] connects different networks over a large geographical area, in order to be employed simultaneously by multiple users according to an on demand service model.

The *Mobile and Distributed Systems Lab (MDSLab)* at the *University of Messina, Italy,* developed *Stack4things*: an

ISSN 2356-5608

OpenStack-based and Cloud-oriented horizontal solution providing IoT object virtualization, customization, and orchestration [12].

The above-mentioned scientific contributions clarify that it is not possible to postpone the correct planning and management of the IoT-Cloud services in industrial plants. In such complex context, it is necessary to use optimized systems addressed to control a multitude of variables thus to avoid low productivity and economic losses. For the above reasons, we describe our strategy in the next Sections.

IV. The IoT-Cloud Brokerage Scenario

In this Section we introduce a description of the real IoT-Cloud Brokerage scenario we refer. It is useful to better understand the proposed strategy and how the simulation tool presented in next Sections works.

In particular, we refer to a dynamic scenario where CSPs are able to share their IoT-Cloud resources among the related Cloud sites (i.e., data-centers) within a cooperative Cloud environment, thus forming a *Community* in order to satisfy what the O&G industries need in terms of *Quality of Service (QoS)*.

In such dynamic critical service-based scenario, an automated *Service Level Agreement (SLA)* negotiation process, which involves both customers and cooperative CSPs , facilitates the bilateral negotiation between the **Community Cloud broker** and multiple providers to achieve the objectives for the O&G industries. Therefore, to relate to each other heterogeneous parameters which are usually considered "singularly" by the IoT-CSPs and to balance them is a challenge. To this end, an approach based on Cloud brokering can simplify the procedures in making the best choice, thus to achieve a good compromise.

The proposed brokerage scenario is exemplified in Fig. 1. It is essentially representative of a large-scale distributed IoT-Cloud platform with a centralized brokerage schema. More

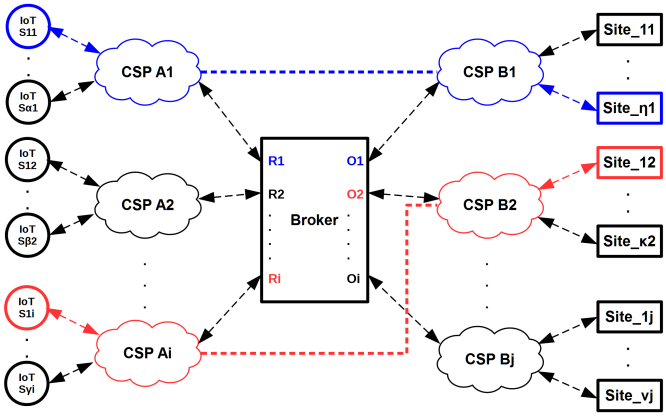

Fig. 1. Exemplifying IoT-Cloud Brokerage Scenario

specifically, on the left, each *Applicant CSPs*, that is unable to serve the IoT services (i.e., in terms of QoS) to a customer through its own Cloud resources, makes a request R to the Broker in order to receive the best offer O from the *Bidder CSPs* on the right. The 'blue' connection int the exemplifying schema reports the CSP A_1 makes a request R_1 to the Broker which, in turn, calculates the best offer among the Bidder CSP. It results in the O_1 from the CSP B_1 which is available to run the IoT services S_{11} at its own $Site\_\eta 1$. Therefore the O_1 is turned by the Broker to the CSP A_1 which attempts to contact the CSP B_1. Finally, the CSP A_1 provides the IoT services S_{11} to the customer, such as the O&G industry, through the CSP B_1 at the Cloud $Site\_\eta 1$. The same approach is for the 'red' connection between the CSP A_i and the CSP B_2. In this case the request R_i for the IoT services S_{1i} can be satisfied by the offer O_2.

V. The MCDM Strategy

The main objective of the proposed Cloud broker decisional system is to pick out a set of offers that meets specific heterogeneous requirements. To this end, our strategy implements a Multi Criteria Decision Making (MCDM) algorithm that has been adapted to address the requirements of the proposed IoT-Cloud scenario using *multi-criteria* JSON Data Sets. In this Section, we present MCDM and discuss how it is adopted to design the multi-criteria decisional system.

The MCDM algorithm allows the Cloud broker to solve a decisional problem in which, according to O alternatives (i.e., offers) and Γ decisional criteria, we have to identify the best alternative or a set of A alternatives so that $2 \leq A \leq \Gamma$. It dynamically manages the alternatives in form of JSON documents as inputs, i.e., each offer is modeled by a JSON document.

The proposed strategy consists of three phases: **preliminary, applicant** and **brokerage**.

A. Preliminary phase

A preliminary phase is under the responsibility of the customer and consists of four main steps.

The **first step** is to choose the set Γ of decisional criteria. The choice implies the following AND condition:

$$AND(c_1, ..., c_N) = true; with\ N \geq 2 \qquad (1)$$

Starting from an in-depth analysis on the IoT-Cloud commercial platforms and services by several "top" leader (e.g., AWS, Teradata, Deloitte US, Google) we choose the following criteria for the proposed MCDM strategy:

- **Operational Availability**;
- **Storage Capacity Service Price**;
- **Data Analytics Service Price**;
- **Cybersecurity Level**;
- **Support Level**;

The **second step** is to quantify, for each criterion, the basic necessities of the IoT-Cloud service to require.

ISSN 2356-5608

Once criteria have been selected, at the **third step**, a weight w is associated with each criterion c, so that:

$$\forall c \in \Gamma \Rightarrow \exists w \in W : \sum_{k=1}^{N} w_k = 1 \tag{2}$$

The **fourth step** is the transmission of the results of the previous three steps to the Community CSP for the next evaluation phase.

B. Applicant phase

The applicant phase is under the responsibility of the Community CSP receiving the request from the customer. In quality of *Applicant CSP* (Fig. 1) it makes a request to the Broker containing all the weighted criteria in the form of *JSON Request Data Set*.

C. Brokerage phase

This phase allows whole Community CSPs to evaluate what is the best Community CSP which is capable to satisfy the request both quantitatively and on a quality level. The Broker broadcasts the request received from the Applicant CSP to the Community CSPs that, in turn, will be able to make one or more offers in quality of Bidders CSPs. Therefore, the Broker: i) gathers the offers for each request, ii) evaluates them by calculating a *score* through the Formula (3), iii) ranks the offers on the basis of the reached scores, iv) share the rank with all of the Community CSPs.

$$score = F_w(w, g, N) = \frac{\sum_{k=1}^{N}(w_k * g_k)}{N * \sum_{k=1}^{N} w_k} \tag{3}$$

More specifically, the score is calculated by multiplying the weight w and the evaluation *grade (g)* assigned to each *k-th* criterion and by normalizing it on a *zero-to-one* rankings. The brokerage phase dynamically runs at Broker, thus allowing it to provide near real-time rankings for each request.

D. Criteria

1) The Operational Availability (A_0) Criterion: We refer to the Operational Availability as the percent of time the IoT-Cloud equipment is available to for use, i.e., it works properly when it is required. Essentially, the A_0 represents the *uptime* of the offered service by the CSP and considers the effect of *reliability, maintainability*, and of the *Mean Logistics Delay Time (MLDT)*. It may be calculated by dividing the *Mean Time Between Maintenance (MTBM)* by the sum of the *MTBM*, the *Mean Maintenance Time (MMT)*, and the *MLDT* as follows:

$$A_o = \frac{MTBM}{MTBM + MMT + MLDT} \tag{4}$$

2) The Storage Capacity Service Price (S_{price}) Criterion: Monetary cost is a quantifiable criterion that addresses customers and organizations in their business. Usually a company which needs to control the production cycle of a plant by a *smart objects network* requires an IoT-Cloud service taking into account the required number of messages to manage (i.e., million of messages) and the related service price generally expressed in $\$/M$ (i.e., dollars-per-million of messages). In particular O&G company generally needs the management of several Tera Bytes (TB)-per-year of data due both to the complexity and magnitude of its plants. Therefore, it should make certain of CSPs assure the adequate *storage capacity*, furthermore with supportable monetary cost. For example, *Amazon Web Services (AWS)* has built IoT specific services (i.e., AWS Greengrass and AWS IoT) based on the above specifications. On the other hand, Bidder CSPs generally offer a "customized volume pricing" which takes into account both the amount and the typology of data to store and to manage.

By specifically referring to IoT services, the Storage Capacity Service Price (we label as S_{price}) is generally expressed in $\$/TB$ (i.e., dollars-per-Tera Byte). A customer (e.g., O&G company) which want to quantify basic TB necessity before making a service request to a Community Cloud member (e.g., via web interface) should consider the following Formula:

$$\begin{aligned} TB &= F_b(Obj_{num}, M, p_{size}, \Delta_t) = \\ &= Obj_{num} * M * p_{size} * \Delta_t \end{aligned} \tag{5}$$

where Obj_{num} is the number of smart objects providing data through the Internet. M is the number of messages-per-hour to manage. The p_{size} parameter indicates the payload size for each message (i.e., byte-per-message). For example, the use of the *MQ Telemetry Transport (MQTT) protocol* [13] by several "top" CSPs (e.g., AWS) in their offered IoT services results *512 byte* is the maximum payload size for each message. The *running time* Δ_t can be generally expressed as a function of the service start and stop dates, and of the number of years yy, months mm, days dd and hours hh in the service "start-stop" time period, as follows:

$$\Delta_t = F_t(date_{start}, date_{stop}, yy, mm, dd, hh) \tag{6}$$

A yearly (i.e., by considering 365 days) *full-time* maintenance at a capable destination results Δ_t equals 8760 hours.

Once a customer knows its basic TB necessity B, it is able to make its request.

3) The Data Analytics Service Price (A_{price}) Criterion: Data Analytics is the "added value" to the Storage Capacity: as a service it processes raw data and converting it into information useful for decision-making by customers. Bidder CSPs generally offer a "customized volume pricing" ($/TB) which takes into account both the amount and the typology of data to process by using a specific software framework (e.g., the Hadoop MapReduce).

4) The Cybersecurity Level (C_l) Criterion: The growing threat of increasingly sophisticated cyberattacks (i.e., cybercrime) threatens the development of safe Information and

ISSN 2356-5608

Scenarios					
Weights →	**w_1**	**w_2**	**w_3**	**w_4**	**w_5**
Scenario 1 →	**0.2**	**0.2**	**0.2**	**0.2**	**0.2**
Scenario 2 →	**0.1**	**0.1**	**0.1**	**0.6**	**0.1**
Scenario 3 →	**0.1**	**0.4**	**0.3**	**0.1**	**0.1**

Requests (Eq.(5))			
Smart Objects (Obj$_{num}$)	**M [mess/h]**	**p$_{size}$ [B]**	**Δ_t [hours]**
100, 500, 1000	720, 1800	500	8760

Offers	
Bidder CSPs$_{num}$	**Offers$_{num}$**
3÷5	5÷10

TABLE I
SIMULATION-BASED SCENARIOS.

MCDM Simulation Environment					
Criteria →	**c_1**	**c_2**	**c_3**	**c_4**	**c_5**
Labels →	**A_0**	**S_{price}**	**A_{price}**	**C_l**	**S_l**
Units →	**%**	**$/TB**	**$/TB**	**GCI index**	**hh**
grade=1	99.95	41÷50 k	5 k	0.000÷0.199	19÷24
grade=2	99.96	31÷40 k	4 k	0.200÷0.499	13÷18
grade=3	99.97	21÷30 k	3 k	0.500÷0.699	5÷12
grade=4	99.98	11÷20 k	2 k	0.700÷0.749	2÷4
grade=5	99.99	1÷10 k	1 k	0.750÷1.000	≤1

TABLE II
SIMULATION ENVIRONMENT. SELECTED RANGE AND GRADE FOR EACH MCDM CRITERION.

Scenario 2; Obj=500; M=1800; p$_{size}$=500 B; TB=3.58							
CSP	**Off**	**A_0**	**S_{price}**	**A_{price}**	**C_l**	**S_l**	**Score**
id	**id**	**%**	**$/TB**	**k$/TB**	**GCI**	**hh**	**0÷1**
1	**4**	99.97	31 k	1 k	0.824 US*	18	**0.84**
3	**2**	99.95	35 k	1 k	0.735 NO*	7	**0.7**
3	**1**	99.95	31 k	1 k	0.706 IN*	20	**0.66**
2	**4**	99.98	22 k	4 k	0.559 MA*	11	**0.6**
4	**1**	99.96	39 k	2 k	0.500 RU*	24	**0.54**

**US=USA; NO=Norway; IN=India; MA=Morocco; RU=Russian Federation*

TABLE III
A LIST OF SAMPLES RESULTING FROM THE J2CBROKER SIMULATION.

Communication Technologies globally. This is a problem for the growing use of IoT, especially in complex environments such as the O&G plants. Safeguarding IoT-Cloud provides for a reliable environment critical for organizations and individuals to conduct business and freely communicate. Based on the above considerations, the proposed strategy includes the Cybersecurity Level as criterion, by referring to the geographical *Global Cybersecurity Index (GCI)* annual report by both ITU and ABI Research [14].

5) The Support Level (S_l)Criterion: Support Level is indicative of the CSPs *problem solving capability*, that is how much time (hours) the CSP needs to solve a problem communicated by the customer, once the support terms specified in the service agreements are activated.

VI. CASE OF STUDY

In order to prove the goodness of the proposed MCDM strategy, we set up the introduced simulated IoT-Cloud brokerage scenario by using the *J2CBROKER* tool [15] on a *Virtual Machine* equipped with *Ubuntu Server 14.04* and hosted in a *IBM BladeCenter LS21* at the *Cloud Laboratory Data-center - University of Messina*.

J2CBROKER is essentially designed on a JAVA client-server architecture which models both the IoT-Cloud service requests and offers (i.e., *Data Sets*) through JSON documents. It executes the calculations introduced in Section V and shows the results (i.e., the Community Bidder CSPs offers) in form of rankings.

A. Simulation Environment

As reported in Table I: i) we modeled three scenarios based on different weights distributions for the selected five criteria and different typologies of requests; ii) each request includes the number of smart objects Obj_{num}, the message-per-hour M to manage, the payload size p_{size} and the the service start-stop time period Δ_t; iii) the Bidder CSPs ranges from 3 to 5 in number and it is able to present offers ranges from 5 to 10 in number. Tab. II shows the selected range and grade for each MCDM criterion.

B. Results

Table III shows a ranking of samples resulting from the *Scenario 2* (Table I). The ranking includes the offers matching the *request* for 500 *Smart Objects* which produce 1800 message-per-hour with a p_{size} of 500 Byte. The "best offer" is the number 4 by the CSP number 1 at a Cloud site which is located in the United States (US). The "total" monetary cost for the proposed IoT-Cloud service is 32 k€/TB due to the sum of the S_{price} and the A_{price}, i.e., 114.56 k€, in order to manage 3.58 TB in a time period of 8760 hours.

Figure 2 shows a linear diagram which represents a set of 30 offers referred to the Scenario 1. For each offer, it reports the *Score* and the quality index related to the Storage and Data Analytics Service Prices. This quality index is calculated as follows:

$$Q = F_q(S_{price}, A_{price}) \quad = 1 - \frac{S_{price} + A_{price}}{S_{priceMax} + A_{priceMax}} \tag{7}$$

The graph allows a clear visualization of the best offers. Based on the Score value, the best offer is the number 5 by the CSP 4 at a destination site which is located in Australia. Based on the Q value, the best offer is the number 1 by the CSP 3 at a destination site which is located in Canada.

By taking into account the same set of offers previously considered, Figure 3 reports, for each offer, the related *Score* and the Cybersecurity Level. Based on the Score value, the best offer is the number 2 by the CSP 2 at a destination site which is located in Canada. Based on the Cybersecurity Level, the best offer is the number 3 by the CSP 1 at a destination site which is located in the United States (USA).

Figure 4 reports the related *Score* and the Cybersecurity Level for 30 offers with reference to the Scenario 2. Based on

ISSN 2356-5608

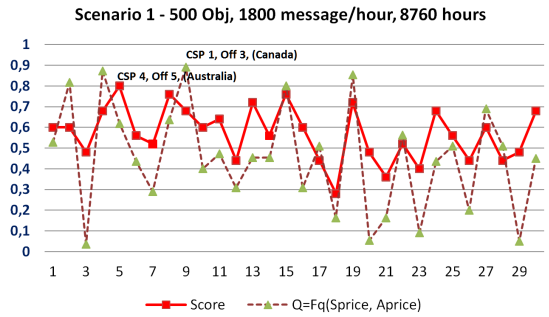

Fig. 2. Comparison between Score and Q for a set of 30 offers in the Scenario 1.

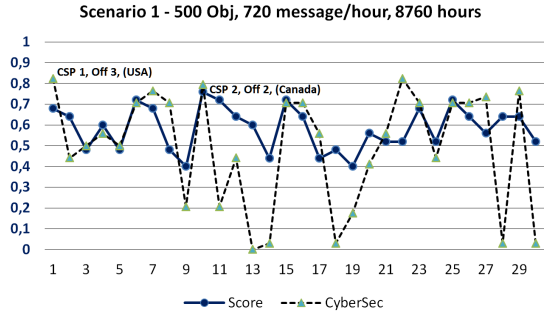

Fig. 3. Comparison between Score and Cybersecurity Level for 30 offers in the Scenario 1.

the Score value, the best offer is the number 1 of the CSP 4 in USA. The graph highlights how the matching between the Score and the Cybersecurity lines is more accurate than the Scenario 1. This result occurs because the requested weight for the Cybersecurity criterion is the highest one (0.6) among all the other criterion weights (0.1).

Moreover, if we evaluate the presented offers only on the basis of the criterion 4, the Cybersecurity line highlights two worst offers. Otherwise, by weighting these latter through all the heterogeneous criteria, they do not represent the worst cases.

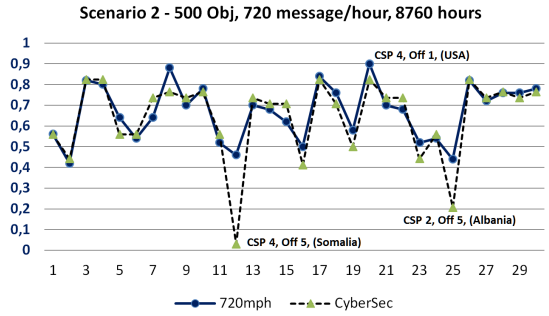

Fig. 4. Comparison between Score and Cybersecurity Level for 30 offers in the Scenario 2.

VII. Conclusion and Future Work

In this paper, a simulation-based *Multi Criteria Decision Making (MCDM)* strategy has been presented in order to help CIOs and IT leaders towards a strategic perspective to capture business value from the IoT-Cloud union.

The result is to allow cooperative small-medium size IoT Cloud providers to satisfy the request for IoT-Cloud services, with a good compromise between service level and business for the O&G industries.

In future work we will integrate the proposed MCDM strategy in the *Stack4Things* framework developed at the University of Messina, by a "MCDM engine" able to achieve an IoT-Cloud brokerage framework.

Acknowledgment

This work was partially supported by EU H2020 BEACON Project G.A.644048, 2015-2018.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Comp. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] K. Dolui, S. Mukherjee, and S. Datta, "Smart device sensing architectures and applications," in *International Computer Science and Engineering Conference (ICSEC), 2013*, Sept 2013, pp. 91–96.

[3] M. Giacobbe, A. Celesti, M. Fazio, M. Villari, and A. Puliafito, "A sustainable energy-aware resource management strategy for iot cloud federation," in *2015 IEEE International Symposium on Systems Engineering (ISSE)*, Sept 2015, pp. 170–175.

[4] S. Murugesan and I. Bojanova, *Community Clouds*. Wiley-IEEE Press, 2016, pp. 744–.

[5] Cisco Global Cloud Index: Forecast and Methodology, 2015/2020.

[6] J. Jung and B. Song, "The possibility of wireless sensor networks for industrial pipe rack safety monitoring," in *2014 47th Hawaii International Conference on System Sciences*, Jan 2014, pp. 5129–5134.

[7] G. Arnold, "Intelligent systems: A new industrial revolution [viewpoint]," *IEEE Electrification Magazine*, vol. 4, no. 1, pp. 64–63, March 2016.

[8] Y. Bao, L. Ren, L. Zhang, X. Zhang, and Y. Luo, "Massive sensor data management framework in cloud manufacturing based on hadoop," in *Industrial Informatics (INDIN), 2012 10th IEEE International Conference on*, july 2012, pp. 397 –401.

[9] Y.-S. Chen and Y.-R. Chen, "Context-Oriented Data Acquisition and Integration Platform for Internet of Things," in *Technologies and Applications of Artificial Intelligence (TAAI), 2012 Conference on*, nov. 2012, pp. 103 –108.

[10] M. Yuriyama and T. Kushida, "Sensor-cloud infrastructure - physical sensor management with virtualized sensors on cloud computing," in *13th International Conference on Network-Based Information Systems (NBiS), 2010*, Sept 2010, pp. 1–8.

[11] S. Madria, V. Kumar, and R. Dalvi, "Sensor Cloud: A Cloud of Virtual Sensors," *IEEE Software*, vol. 31, no. 2, pp. 70–77, Mar 2014.

[12] G. Merlino, D. Bruneo, S. D. Stefano, F. Longo, and A. Puliafito, "Stack4Things: Integrating IoT with OpenStack in a Smart City context," in *Proceedings of the 2014 International Conference on Smart Computing Workshops (SMARTCOMP Workshops)*. Hong Kong, China, 5 November 2014: IEEE Computer Society, 2014, pp. 21–28.

[13] The MQ Telemetry Transport (MQTT) Protocol. http://mqtt.org/.

[14] ABIresearch, *Global Cybersecurity Index & Cyberwellness Profiles Report*, 2015.

[15] M. Giacobbe, R. D. Pietro, C. Puliafito, and M. Scarpa, "J2CBROKER: A service broker simulation tool for cooperative clouds," in *10th EAI International Conference on Performance Evaluation Methodologies and Tools (Valuetools 2016)*, 2016.

ISSN 2356-5608