Interoperability for the sustainability assessment framework in IoT like environments

Valentina Timčenko, Nikola Zogović, Borislav Đorđević

School of Electrical Engineering, Institute Mihailo Pupin, University of Belgrade, Belgrade, Serbia

{valentina.timcenko, nikola.zogovic, borislav.djordjevic}@pupin.rs

Abstract— **Internet of Things (IoT) as a concept provides a possibility of interconnecting different devices and technologies through the Internet. Such diversity of devices and heterogeneity of the communication protocols, data formats and service demands for storage, energy, and availability has imposed a huge set of side effect issues that are becoming the serious stumbling stone in IoT-like system design and management. In this paper we have put interoperability in the center of our attention as one of the most persistent issues, making an effort to enhance the multi-objective cloud computing sustainability assessment framework by providing the necessary level of sustainable interoperability for IoT environments.**

I. INTRODUCTION

The advent of Cloud Computing (CC) and Internet of Things (IoT) merging concept provides the most potential transformative paradigm with tempting opportunities that are offered in business and society areas. It brings a number of computing services as a response to the challenges for providing different usage alternatives to both end users and operators. Considering its rising application, IoT-on-Cloud draws strong efforts hype in conforming needs for assessing proper sustainability model that would be adequate for such a modern and vivid technological development.

Our research background in the area of the sustainability assessment for CC and IoT has motivated us to proceed with further step towards expanding the framework and estimate the impacts of the interoperability as one of the sustainability objectives [1, 2, 3]. Interoperability reflects the continual capacity of a system to provide and use different business/technological services from or to a different system and consequently the exchange of data with other systems in order to achieve some defined purpose in a specified environment. The sustainability, supported through four defined pillars, allows the provisioning of different interoperability flawors. In this paper the spotlight is on the business pillar, nowel sustainability awareness area introduced by the aforementioned Multi-Objective Cloud Computing (MO CC) Sustainability Assessment Framework [1-3]. We reffer to the sustainable interoperability in a broader context, considering that there are many factors that contribute in different manner to the global functionality of the system/enterprise/organization or to the user quality of the experience (QoE).

II. RELATED WORK

The idea of merging and efficiently using the IoT-on-Cloud paradigm benefits has raise the interest in different application fields. It has found a place in the energy management infrastructures providing flexibility for better optimization of the smart sensors geographical distribution [4] a sensing as a service paradigm is used as a base for trading-based value creation model for efficient adoption of IoT in society, thus forcing the sustainable adoption of IoT for fulfilling the social aspects and needs. The need for secure and personalized use of IoT components and services has inspired a number of research groups to confront the needs and possibilities in a way to grant IoT security by providing strong topological sustainability [5]. In order to deeply explore the vision of IoT development in the context of the use of additional systems and platforms such as CC, the major efforts are focused towards a range of possible applications, deal with all the challenges, and use all available opportunities and benefits that such a merging provides [6]. The strong sustainability approach is a must have for proper operation of any such system and for the provisioning to the user all the necessary conditions and services. The United Nations sustainability model is one of the most respectful studies related to the sustainability development modeling, which also supports the open data initiative [7, 8, 9, 10]. It defines a set of 10 principles and 17 sustainability development goals (SDGs) from three defined categories: economy, ecology and social. For further boosting of the importance of such an approach, we have proposed a framework, MO CC Sustainability Assessment model, that brings enhancement in terms of additional line of consideration, the business area. This framework is foreseen to allow to the users constrains-free area when selecting significant objectives for their system/working platform. It provides additional design flexibility for joint use of CC and IoT concepts. The main goal of this paper is to provide more details related to technical characteristics of the sustainability provisioning in IoT, targeting exclusively the interoperability issues.

III. INTEROPERABILITY IN IOT ENVIRONMENTS

The versatility and omnipresence of the IoT has roughly defined two categories of supportive technologies, short and long range technologies.

The short range technologies are exploited mostly in low cost and low power/energy consumption environments, where the main representatives belong to LAN/PAN technology type (e.g. Bluetooth BLE, WiFi,

ZigBee). The long range technologies deal with high cost and high power consumptions, covering mostly the 3GPP technologies such as LTE, CatM/NB-IoT. Nevertheless, the IoT technological bum has raised lots of challenges making the choice of the base technology a complex problem to analyse. This oversimplified classification does not follow the realistic view of new generation propositions that are circling in the middle ground between these two groups of technologies. The appearance of the low power wide area network technologies (LPWAN) has brought a new flawors of possibilities, where the main representatives are: Sigfox (ultra narrow band), LoRa, and NB-IoT.

In Industrial IoT, the devices are mostly used for industrial automation processes which require direct connection to a power supply and high data rate, while the IoT infrastructure requires an end-to-end security across the protocol stack. Thus, the main question is which connectivity protocol most closely meets the technical requirements for a specific IoT space, whereas we additionaly consider the sustainability of such interoperability demanding environments.

The general conceptual interoperability layering model offers the possibility of providing granularity to the interoperability aspect of the system as a whole (Figure 1).

Fig.1 aids in understanding the interoperability through levels, starting from the basic "technical level", to the most complex - "conceptual interoperability" (providing the meaningful abstraction of the reality).

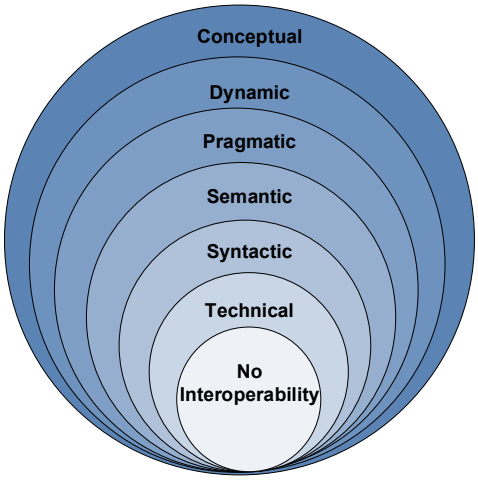

Figure 1. Levels of the conceptual interoperability model

Our focus is on the technical interoperability characteristics. It is associated with hardware and software components, systems and platforms that enable Machine-to-Machine (M2M) communication. It is related to the protocols and the infrastructure necessary for their proper interconnection and operation. The TCP/IP protocol stack is a generally accepted concept in system networking and interaction, although recently some new tendencies have appeared, such as DASH7 (representing the Low Power Wireless IoT Stack) [11]. Yet, there is no apparent move towards the so needed integration and consolidation of IoT wireless technologies. When combined with the increasing trend of the system vulnerabilities and security concerns, the issue with proper protocol layering is deepened to the inevitable introduction of a range of security protocols and crypto features. Thus, the fundamental interoperability relies on the compatibility/understandability of the used encryption algorithms, and successful secure keys exchange.

A number of social, ecology care, financial, organizational, and legal organizations and government bodies are cooperating in order to define the set of critical points that would tackle common interest and/or information exchange for overall benefit. The request for such a cross-domain interoperability provisioning has raised the question of its proper implementation to the proposed MO CC Sustainability framework, assuming diversity of technologies used at different system/network layers, and focusing mostly on business area and IoT environment [1, 2, 12]. The proposed framework is also covering the open data paradigm as one of the main cornerstones for interoperable sustainability of the system. The sustainability need for openness of the data sources, being private, public or of other type is equally important for interoperability provisioning [13]. Figure 2 provides details related to the business pillar of the MO CC Sustainability Framework.

MO CC Sustainability Framework encompasses four sustainability pillars: economy, ecology, social and business (UN supports the first three). Interoperability provisioning issue tangles in different ways the four defined sustainability pillars and in broader context, interoperability is related to many factors that contribute in different manner to the global functionality of the system/enterprise/organization or to the user quality of the experience (QoE). One of the reasons of its introduction to the overall sustainability framing and its analysis is the need to provide interconnectedness of mutually coherent systems, keeping in line with the quest for efficient, fast, superpower systems that would smoothly give necessary level of quality of service (QoS) to the end users, energy and storage efficiency to the providers, and keep good balance of the cost satisfaction to both users and provides. The complete framework is explained in [1, 2, 3].

As the 3rd Generation Partnership Project (3GPP1) claims, the “Interoperability is the ability of two or more systems or components to exchange data and use information“ [14], this definition enforces the issues related to the data flow and targets the most common IoT common challenges. In general the interoperability is "the ability of two systems to interoperate using the same communication protocol” mixed with "the ability of equipment from different manufacturers (or different systems) to communicate together on the same infrastructure (same system), or on another while roaming" [15, 16], and we consider these as definitions for our further use. Thus, taking into consideration the clauses related to the technical interoperability we are providing a survey on interoperability measurement as an enhancement to the proposed sustainability assessment framework, covering the business pillar features with necessary interoperability functionalities.

It relies on the definition of the additional decision variables and objectives that would involve the interoperability aspects that are in line with the sustainability assessment area.

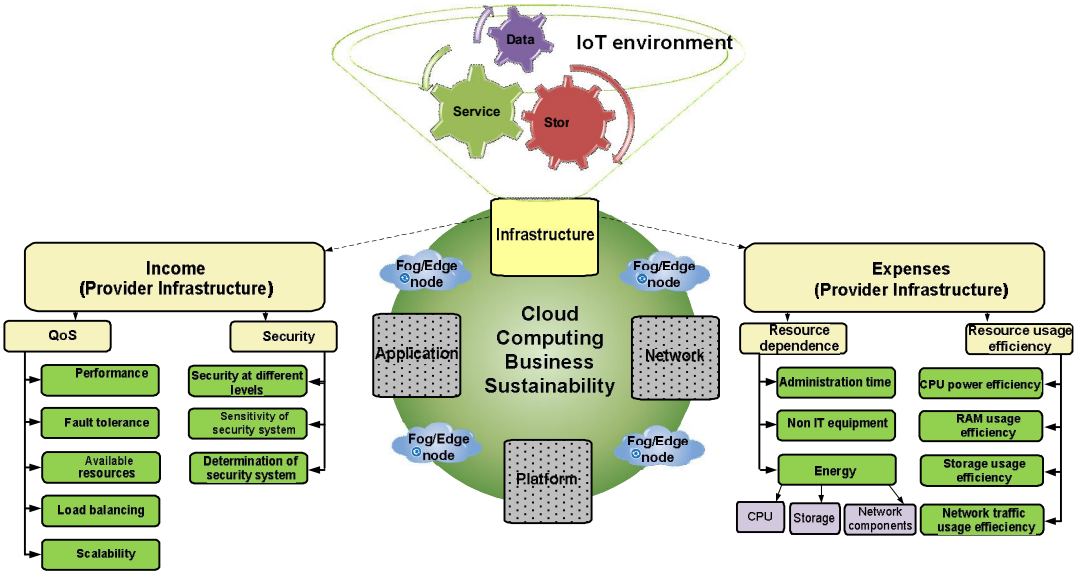

Figure 2. IoT-to-Cloud business pillar of MO Sustainability Framework

Definition of the sustainability from the interoperability point of view covers in more detail the security concerns. Security at different IoT TCP/IP protocol stack levels significantly influences the technical interoperability.

IV. INTEROPERABLE IOT SUSTAINABILITY

Undoubtedly, interoperability stands for an unavoidable characteristic to fulfill if there is an aim to provide sustainable functioning of any system or next generation network [17, 18]. One of the reasons of its introduction to the overall sustainability framing and its analysis is the need to provide interconnectedness of mutually coherent systems, keeping in line with the quest for efficient, fast, superpower systems that would smoothly give necessary level of quality of service (QoS) to the end users, energy and storage efficiency to the providers, and keep good balance of the cost satisfaction to both users and provides. From the sustainability point of view, the question of providing interoperability in IoT like environments (enterprise information systems, smart homes, intelligent transportation systems, smart grids, virtual power plants, energy management systems, intelligent health monitoring systems, smart cities, etc.) goes much further than solving the technological issues, and it covers intensively the social, economy, ecology, organizational and in some aspects political factors that impact system to system performance bringing to the users more freedom and a higher quality of life (QoL) [19]. These conditions and requests require the use of the open data sources (private, public). The open data paradigm is one of the main cornerstones for interoperable sustainability of the system [20].

The goal is to support the IoT system sustainability by responding adequately to the task of building coherent and interoperable services, when the individual components/devices are technically different and managed by diverse enterprises, users or organizations.

An idea of the integrative and sustainable approach can be explained by, for example, the enforcement of the use of the identical or compatible operating systems (Unix, Linux, Windows, etc). Instead, the network itself can provide an integrative mechanism using identical protocols, according to some specified protocol stacks. The technological challenges in communication can be described through research initiatives for exploring the possibilities of integration, interconnection and interoperability of IoT technologies and systems [21]. The communication is of the highest concern as IoT allows for heterogeneous environment in the sense of devices, services, and communication media. In [12] the spotlight is on the issues of integration of existing protocols and technologies, scalability for new ones, keeping a good balance with the pervasiveness, context-awareness and security for IoT environments. The protocol non interoperability can be explained through a range of real time cases, where e.g. the diversity of the incompatible characteristics and demands for proper functioning of the file sharing protocols (FTP (File Transfer Protocol), NFS (Network File System), SMB (Server Message Block, Microsoft compatible), and SCP (Secure Copy Protocol) used on the application layer can actually disable the communication. NFS is typically used by the UNIX community and is not compatible for the MS Windows family users, while SMB stand for the MS Windows FSP and is formally no understandable for UNIX community. On the other hand, the Linux community supports both protocol types. FTP has also an open non-crypto version, and different cryptographically secured adaptations, which can additionally complicate the issue of algorithms mutual compatibility and proper key exchange between entities. Fig. 3 provides an overview of protocol stack generated based on the TCP/IP concept and modified according to the IoT specifications. The five basic layers (PHY, DataLink, Network, Transport, and Application) are mutually interlaced and are tailored to keep the conformity for providing necessary conditions for different technologies that are using several layers at the same time.

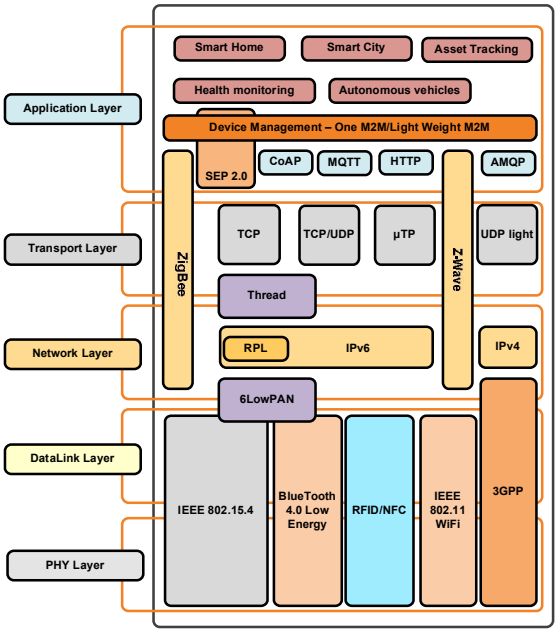

Figure 3. IoT enhanced TCP/IP stack [22]

This approach has been supported by many organizations as the basis for creating large corporate networks. Finally, interoperability can be achieved by using the application software generated to be operational on different platforms. As the practical reach of our interoperability goal is to provide the level 1, so called "technical interoperability" in accordance to the proposed MO CC sustainability concept, we are questing the capabilities of the communication infrastructure, generally basing the approach on the estimation of the interoperability achievements in the area of the network connectivity and functionality of the communication protocols at different IoT TCP/IP protocol stack layers of the considered network, organization or system (Fig. 3). The main focus of the recent research efforts is on the application layer.

The proper IoT system functionality is potentially complicated by systems vulnerabilities to a range of cyber attacks, hence the need for security on all the layers of data/information transmission is being highly raised. It is also a foundation for architecture and functioning of a range of security protocols related to different stack layers. Their main characteristics is the introduction of the crypto features, whereas the fundamental interoperability relies on the compatibility/understandability of the used encryption algorithms, along with the successful and secure keys exchange.

The general impresion is that there is a strong need for detailed and comprehensive standardization, in order to regulate the complex and messy results of the IoT revolution. The standardization is the main catch when considering issues with IoT like environments, and mostly targets de facto protocol layering and their interconnection in the system as a unit and on the intersystem level [23]. When tackling the characteristics of the adopted version of TCP/IP protocol landscape this idea is further elaborated, reaching the more fragmented structure shown in Fig. 4. The aim is to provide an approach to the problem of assuring the technical interoperability in the context of the needed sustainability assessment for the network/system. We stick to the design and implementation of sustainable high tech environments in order to allow their technological evolvement into the secure, resource management efficient, and intelligently managed systems that would provide:

- The proper approach to the issue of embedding various IoT layer protocols into TCP/IP stack interoperability formalism. The proposed MO CC sustainability framework and its business sustainability pillar covers the integration of the interoperability features that allow sustainable functioning of the system as a whole, perfectly integrating IoT with Cloud based backend. For proper approach to the interoperability assessment it is necessary to consider the specificity of individual layers and their protocols.

- Definition of the rules/specifications to keep the necessary interoperability level while implementing security protocols. The additional goal is to keep assuring the privacy and security on various layers of protocol stack. The main concern is the mutual compatibility/comprehensibility of algorithms and adequate key exchange between the entities. It is important to find the adequate position of such a stack from the information technological point of view as well from the enterprise (business) perspective. To allow sustainable interoperability and make everything function as intended, there are some business values to follow [24]:

  1: Device management procedures encompassing: the proper service provisioning, user/client registration, firmware management, remote access management, asset structure consolidation, guaranteed security and privacy;

  2: Business procedures for Service Transformation: providing a range of support services for smart devices, providing marketing documentation and procedures for the owners and vendors of smart devices, keeping an eye on the possible impact on manufacturing for devices through efficiency calculations;

  3: Analytics services and procedures are mostly based on the application of the machine learning and artificial intelligence techniques in order to provide information on: the impact of used technologies for the data collection, efficiency of the data mining techniques, visualization possibilities and details.

Figure 4, although not being exhaustive as this is mission impossible with every new device that appears on the market on daily basis, provides a basic overview of the situation at the moment. With to many protocols, need for keeping layering the stack in order to be neat and precise still gives an impression of a mess, but controlled one. The advantage of this proposal is the positioning of a new layer that is business oriented, covering specifics that are necessary for healthy development of the modern enterprises.

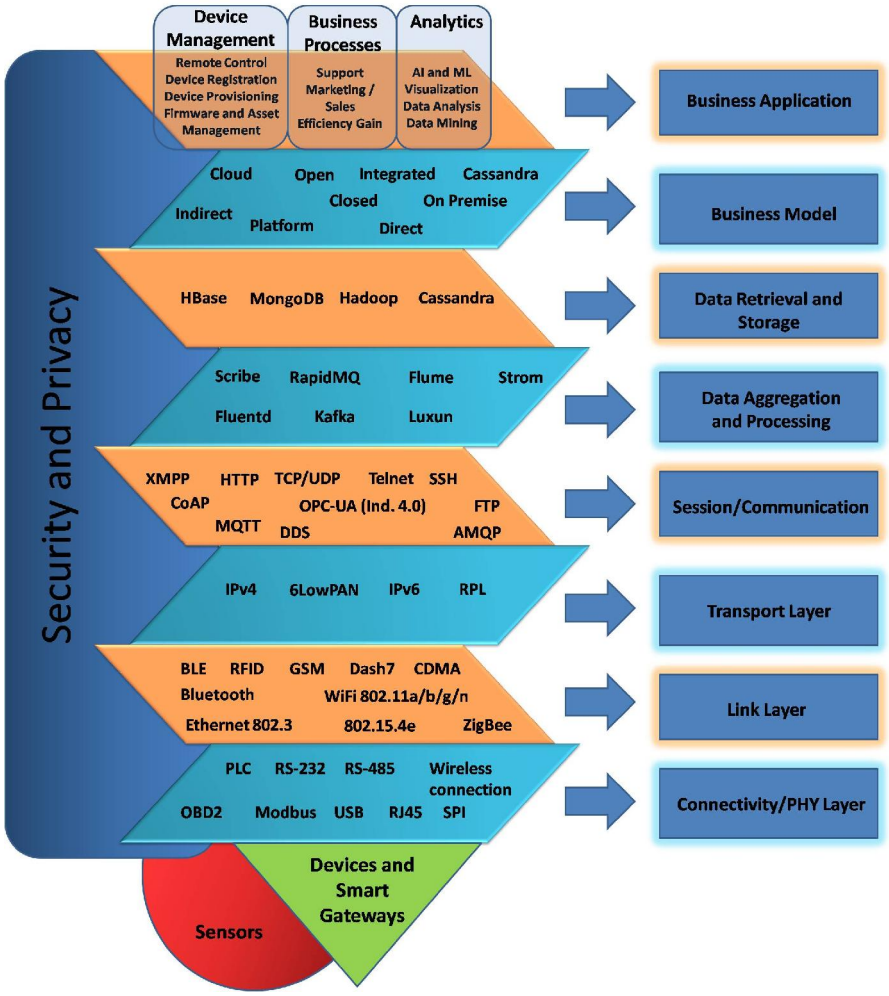

Figure 4. IoT protocol landscape [24]

Goal O_1	QoS maximization	$O_1 = \max QoS(S_i, VM_j) = \max f(QoS\_DesignVariables)$ $QoS(performances) = f(I_{qf}, \Pi_{qf}, S_i \leftrightarrow VM_j, VM_j(S_i \rightarrow S_k))$
Goal O_2	Sensitivity maximization	$O_2 = \max TP_{rate}(TP_{rate\_i})$
Goal O_3	Specificity maximization	$O_3 = \max TN_{rate}(TN_{rate\_i})$
Goal O_4	Resource use efficiency maximization	$O_4 = \max \varphi_1(S_i, VM_j)$ $\varphi_1(S_i, VM_j) = \frac{1}{4}\left(\frac{\sum_{j=1}^{N_{VM}} VM_j^{CPU}}{\sum_{i=1}^{NS} S_i^{CPU}} + \frac{\sum_{j=1}^{N_{VM}} VM_j^{RAM}}{\sum_{i=1}^{NS} S_i^{RAM}} + \frac{\sum_{j=1}^{N_{VM}} VM_j^{str}}{\sum_{i=1}^{NS} S_i^{str}} + \frac{\sum_{j=1}^{N_{VM}} VM_j^{bw}}{\sum_{i=1}^{NS} S_i^{bw}}\right)$
Goal O_5	Minimization of the number of migrations of virtual machines	$O_5 = \min \varphi_2(VM)$, $\varphi_2(VM) = \sum_{j=1}^{N_{VM}} VM_j(S_i \rightarrow S_k)$
Goal O_6	Minimization of CPU energy consumption	$O_6 = \min P_{CPU}$, $P_{CPU} = \sum_{i=0}^{N_{CPU}-1} \sum_{j=0}^{N_{CPU\_st}-1} \alpha_{i-j}^{CPU} * P_j^{CPU}$ $\alpha_{i-j}^{CPU} = f(Hypervisors_{type}, CPU_{sch}, S_i \leftrightarrow VM_j), VM_j(S_i \rightarrow))$
Goal O_7	Storage power consumption minimization	$O_7 = \min P_{str}$, $P_{str} = P_{HDD} + P_{SSD}$
Goal O_8	Energy efficiency maximization	$O_8 = \max EE$, $EE = \frac{QoS}{P}$
Goal O_9	Maximization of the storage energy efficiency	$O_9 = \max EE(str)$, $EE(str) = \frac{QoS(str)}{P_{str}}$
Goal O_{10}	Maximization of the networking energy efficiency	$O_{10} = \max EE(networking)$, $EE(networking) = \frac{QoS(networking)}{P_{networking}}$
Goal O_{11}	Maximization of secure interoperability	$O_{11} = f(Key\ Management,\ Encryption/Decryption\ algorithms,\ Identity\ checking\ mechanisms)$

Figure 5. Set of goals to fulfill IoT business sustainability principles [1, 2, 3]

It is tailored according to the needs of business/enterprise environment that supports the need for connecting the devices with some business value. Interoperability is defined as a Goal 11 in the defined set of goals to fulfill the sustainability assessment framework (Fig. 5). The O_{11} defines the maximization of secure interoperability. It is derived from the fact that the security at different IoT protocol stack levels significantly influences the fulfillment of the technical interoperability.

$$O_{11} = f(KeyMngm, Encryption/Decryption, IDcheck) \quad (1)$$

The Goals O_2 (sensitivity maximization) and O_3 (specificity maximization), which are directly related to the security, have great impact to the Goal O_{11}, but also to other goals, such as Goal O_1 (QoS Maximization). This impact is foreseen as with negative and positive tendencies. The negative impact is to the performances as when searching for higher level of security goals there are always additional procedures, system CPU and storage overloads and delays. The positive impact targets better confidentiality reliability, authentication, integrity, and non repudiation.

For comprehensive interoperability consideration, we can even define the apsolute and relative interoperability.

Let S be a set of all the possible features related to analyzed IoT technologies. Let N_s be the cardinal number of the set S. The technology X (e.g. WiFi) supports certain set of features N_{WiFi}, while some other technology (e.g. ZigBee) provides info on N_{ZB} properties. There is a possibility that different technologies have a subset of identical features.

The absolute interoperability I_A of certain technology is defined as a ratio of a number of features supported by that technology and the total number of features provided by a set of observed technologies, S, and I_A values belong [0, 1] range. E.g. WiFi has I_A defined as N_{WiFi}/N_s, while for ZigBee it is N_{ZB}/N_s.

The relative interoperability I_R of technology A to the technology B is the ratio of the number of features that are supported by both technologies and the number of properties supported by technology B.

These calculations can be based only on the defined spectrum of features. Thus, for the case of the interoperability there is need to consider among others, the features that are correlated to our Goal 11.

Thus there is need to examine IoT system performance against the following set of characteristics:

- Confidentiality: preventing unauthorized access to information, while providing message exchange privacy
- Integrity: prevention from unauthorized change of information, while providing the confirmation that the messages are unchanged during the exchange
- Availability: prevention from unauthorized disabling of the access to the information or resources
- Authentication: prevention from false representation, (identification of message sources and verification of person's identity)
- Non repudiation: prevention of the false repudiation to sending certain message/file (it can be proven that a message/document comes from a given entity, although that entity denies it).

Additionally, such a secure interoperability is further enhanced with cryptographic features [25]. The cryptographic systems form a part of an integral security provisioning system. It relies on five-tuple (M, C, K, E, D), namely: set of messages, set of ciphers, set of keys, encryption and decryption functions. The need for proceeding with encryption and decryption (relation 2) of the messages during the exchange brings additional delay in the processing, resulting in decrease of the general system performances from the cost/price/time point of view.

$$T_{T'} = T_{Encryption} + T_{CypherMessage} + T_{Decryption} \quad (2)$$

where T_T stands for the time needed for the transmission, $T_{CypherMessage}$ is the time that is calculated as a function based on the additional data related to the introduction of the ciphers, and also depends on the network traffic load at the moment of the evaluation.

The delay that crypto graphical operations introduce into the calculations can be approximated to:

$$T_{T'}/T_T = T_T/T_{Encryption} + T_{CypherMessage} + T_{Decryption} \quad (3)$$

For gaining proper and sustainable interoperability, inter alia, there is need for enhancement of the procedures and algorithms that are related to mentioned security methods. Also, there is need to be in line with the absolute and relative interoperability when choosing the proper protocols and technologies for the IoT environment under the consideration. These techniques can significantly differ depending on the technology and its standard and practices.

V. CONCLUSION

IoT technologies have become an integral part of modern human life. It is already covering different areas related to comfortable and quality living, while on the other side it is highly incorporated into different business and industrial applications. Thus, we are facing the rising needs for the efficient, smart and green application of IoT: for smart cities, agriculture, automotive industry, health care, government and administration, retail procedures, asset traking applications and a range of other possible application. Still, the main challenge is if IoT can flourish under the weight of the rising expectations? The huge number of different technologies, protocols, and constant need for their interconnection requires for proper standardization in order to allow sustainable interoperability level in such messy environments. The weak environmental characteristics, low compatibility, weak ciphers, delays in encryption/decryption, filesystem authentication incompatibility, traffic analysis algorithms, and roaming are just some of the main issues to deal with in this process. In order to provide fast, secure, low noise, highly energy, storage and CPU efficient, smart IoT technologies we have proposed a multi objective cloud

computing sustainability assessment framework. The 11 defined goals are tailored with a special focus to the business area and its weakest points, the QoS performance, security, storage and memory management, and interoperability.

ACKNOWLEDGMENT

The work presented in paper has partially been funded by the Ministry of Education, Science and Technological Development of Republic of Serbia: V. Timčenko by grants TR-32025/TR32037, N. Zogović and B. Đorđević by grant III-43002.

REFERENCES

[1] V. Timčenko, "Assessing Cloud Computing Sustainability," In Proc. of the 6th *Int. Conf. on Information Society and Technology*, *ICIST2016,* pp. 40-45, 2016.

[2] V. Timčenko et al, "An IoT business environment for Multi Objective Cloud Computing Sustainability Assessment Framework," In Proc. of 7th Int. *Conf. on Information Society and Technology*, *ICIST2017*, pp.120-125, 2017.

[3] N. Zogović et al, "A Multi-objective Assessment Framework for Cloud Computing," In Proc. of *TELFOR2015*, Serbia, Belgrade, pp. 978 - 981, 2015.

[4] M. Giacobbe et al, "A sustainable energy-aware resource management strategy for IoT Cloud federation," *Systems Engineering (ISSE), IEEE International Symposium on*, 2015.

[5] D. Zegzhda, T Stepanova, "Achieving Internet of Things security via providing topological sustainability," *Science and Information Conference (SAI)*, IEEE, 2015.

[6] S. Chen et al. "A vision of IoT: Applications, challenges, and opportunities with china perspective," *IEEE Internet of Things journal* 1.4, pp. 349-359, 2014.

[7] A report to the SG of the UN by the LC of the SDSN Indicators and a monitoring framework for the sustainable development goals – Launching a data revolution for the SDGs, 2015. Available: http://indicators.report/

[8] The Sustainable Development Goals Report, United Nations, New York, 2017. https://unstats.un.org/sdgs/files/report/2017/TheSustainableDevelopmentGoalsReport2017.pdf

[9] S.88 DIGIT Act: "Developing Innovation and Growing the Internet of Things Act" or "DIGIT Act", enacted by the Senate and House of Representatives of the United States of America in Congress assembled. [Available] https://www.congress.gov/bill/115th-congress/senate-bill/88/text

[10] Y. Lu et al, "Policy: Five priorities for the UN sustainable development goals-comment," Nature 520.7548, pp. 432-433, 2015.

[11] M. Weyn et al, "DASH7 alliance protocol 1.0: Low-power, mid-range sensor and actuator communication," *Standards for Communications and Networking (CSCN), IEEE Conference on*. 2015.

[12] A. Botta et al, "Integration of Cloud computing and Internet of Things: A survey," Future Generation Computer Systems, 56, pp. 684–700, 2016.

[13] M. Gayler,"Open Data, Open Innovation and The Cloud," *A Conference on Open Strategies - Summit of New Thinking*, Berlin, 2012.

[14] H. van der Veer, A. Wiles, "Achieving technical interoperability," European Telecommunications Standards Institute, 2008.

[15] "ETSI TS 102-237-1," Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Interoperability Test Methods and Approaches; Part 1: Generic Approach to Interoperability Testing, 2005.

[16] ETSI "TISPAN NGN Functional Architecture," Section 7 "NGN Interconnection". ETSI ES 282 001 v2.0.0. March 2008.

[17] H. Panetto et al, "New perspectives for the future interoperable enterprise systems," *Comp. in Industry*, 79, pp. 47-63, 2016.

[18] G. Weichhart et al, "Challenges and current developments for sensing, smart and sustainable enterprise systems." Computers in Industry 79 (2016): 34-46.

[19] Z. Milosevic, A. Bond, "Digital health Interoperability frameworks: use of RM-ODP standards," *IEEE 20th Int. Enterprise Distributed Object Computing Workshop (EDOCW),* 2016.

[20] The Global Open Data Initiative (GODI), 2013. Online: http://globalopendatainitiative.org/

[21] R. Gravina et al, "Integration, Interconnection, and Interoperability of IoT Systems," *Springer International Publishing*, 2018.

[22] BUTLER, EU FP7 project, Smartlife – Secure and Context Awareness in the IoT, http://www.iot-butler.eu/

[23] Internet of Things Global Standards Initiative. [Available] http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

[24] A. Passemard, "The Internet of Things Protocol stack–from sensors to business value." online at http://entrepreneurshiptalk. wordpress. com/2014/01/29/the-internet-of-thing-protocol-stack-from-sensors-tobusiness-value (2014).

D. Zegzhda, T. Stepanova, "Achieving Internet of Things security via providing topological sustainability," *InScience and Information Conference (SAI)*, IEEE, pp. 269-276, 2015.