ADVANCE'2021

Zaragoza, Spain
February 2021

9th International Workshop on ADVANCEs in ICT Infrastructures and Services

ADVANCE'2021

9th International Workshop on ADVANCEs in ICT Infrastructures and Services

Zaragoza, 2nd February 2021

Universidad de Zaragoza
University College Cork

9 782956 112846

Picture by Ramón Legarre https://flic.kr/p/5o7mNv under Attribution-NonCommercial 2.0 Generic (CC BY-NC 2.0)

Preface

It is a great pleasure to present you ADVANCE’2021: the 9th International Workshop on ADVANCEs in ICT INfrastructures and Services. This year 2021, it was planned to be held in Zaragoza (Spain), but, unfortunately, due to the world pandemic, it was celebrated online. Perhaps, more than ever, ICT technologies need to play a key role in our societies, as the virus is dramatically limiting our social face-to-face interactions, we need communication technologies to help mitigate our constraints, but also current advances in networking, distributed services and distributed infrastructures can also significantly help manage the sanitary conditions. ADVANCE represents, therefore, a fantastic forum for discussion about how current ICT technologies and their research trends should evolve to meet our current and future emergency needs in the ICT domain.

The focus of the ADVANCE series of workshops is to provide a forum for the publication, presentation and discussion of relevant efforts of the worldwide scientific community, practitioners, researchers, engineers from both academia and industry on the latest theoretical and technological advances in ICT. After the successful organization of the 1st ADVANCE workshop in 2012 in Canoa Quebrada (Brazil) with the support of IFCE Aracati, the 2nd edition was held in the city of Morro de Sao Paulo (Brazil). In 2013, with the support of IFCE, the 3rd edition was held in Miami (USA). In 2014, with the support of IFU, the 4th edition was held in Recife (Brazil). In 2015, with the support of UFPE, the 5th edition was held in the city of Evry Val d’Essonne (France). In 2017, with the support of UEVE/Paris Saclay, the 6th edition of the workshop was held in the beautiful city of Santiago de Chile (Chile), with the support of the Universidad De Chile (UC). The 7th edition was held in Cape Verde Islands with the support of the Universidad de Cabo Verde. In 2020, the 8th edition is being held in the city of Cancun (Mexico) with the support of the Universidad del Caribe and the Universidad Autonoma de Yucatan. Finally, this year 2021, is being held online, with the support of the University of Zaragoza (Spain) and University College Cork (Ireland).

ADVANCE’2021 consists of two main sessions, with two Invited Talks. The technical sessions are addressing currently hot topics, including Service Oriented Computing, Smart Cities, Smart Contracts, Block-Chain technologies and e-Health, Internet of Things and Cloud & Fog computing, and Software Defined Networking (SDN). The 2 Technical Sessions consist of 4 full papers and 4 short papers. The first invited talk about “Artificial Intelligence at the Edge of the Cloud” is given by the invited speaker Prof. Omer F. Rana from Cardiff University (United Kingdom). The second invited talk, about scalability of LoRa Networks for dense IoT scenarios, is given by the invited speaker Prof Congduc Pham from the University of Pau et des Pays de l’Adour (France). An overall number of 10 papers were submitted this year, we want to thank the 26 authors that submitted their papers to ADVANCE’2021. Our deep gratitude also goes to the 34 members of the Technical Program Committee for their hard work in reviewing the submissions. Finally, we thank our colleagues from University of Zaragoza and University College Cork for the organization and making possible the celebration of ADVANCE’2021 online.

Enjoy ADVANCE’2021

Rafael Tolosana Calasanz, General Chair
Gabriel Gonzalez-Castañé, TPC Co-Chair
Nazim Agoulmine, Steering Committee

General Chair

Rafael Tolosana-Calasanz, Universidad Zaragoza, Spain

TPC Co-Chairs

Gabriel Gonzalez-Castañé, University College Cork, Ireland

Steering Committee

Nazim Agoulmine, UEVE-Paris Saclay University, France
Mauro Oliveira, IFCE Aracaxi, Brazil
Paulo Roberto Freire Cunha, UFPE, Brazil
Hakim Abdelhafid, University of Montreal, Canada
Joberto Martins, University of Salvador, Brazil
Neuman De Souza, UFC, Brazil
Karima Boudaoud, University of Nice Sophia-Antipolis, France

Scientific Committee

Wassila Aggoune-Mtalaa, LIST, Luxembourg
Hakim Abdelhafid, University of Montreal, Canada
Hossam Affifi, IMT, France
Nazim Agoulmine, UEVE-Paris Saclay University, France
Domingos Andrade, UNICV, Capo Verde
Jordi Arjona – ITI, Spain
Mustapha Ait-Idir, Banque Nationale du Canada, Canada
Farid Alilat, USTHB, Algeria
Javier Baliosian, University of Uruguay, Uruguay
Luis Basto Díaz, UADY, Mexico
Djamel Belaid, IMT, France
Sonia Ben rejeb-Chaouch, Mediatron-Supcom, ISI, Tunisia
Reinaldo Bezerra Braga, IFCE, Aracaxi, Brazil
Abdelmadjib Bouabdallah, UTC, France
Karima Boudaoud, University of Nice Sophia-Antipolis, France
María Canales – Universidad de Zaragoza, Spain
Carlos-Andre Baptista Carvalho, Federal Univesrity of Piaui, Brazil
Alejandro Calderon – University Carlos III Madrid, Spain
Sandra Céspedes, Universidad de Chile, Chile
Rossana Maria de Castro Andrade, UFC, Brazil
Olfa Chabbouh, Supcom, Tunisia
Nada Chendeb, Lebanese University at Tripoli, Lebanon
Elhadi Cherkaoui, Beamap, France
Emanuel Coutinho, UFC, Brazil
Willie Donnelly, WIT, Ireland
Jean-guy Fontaine, Consultant, France
Paulo Roberto Freire Cunha, UFPE, Brazil
Gabriel Gonzalez-Castañé,University College Cork, Ireland
Miguel Franklin De Castro, UFC, Brazil
Jose Neuman De Souza, UFC, Brazil
Marcelo Anderson Baptista Dos Santos, IF Sertao-PE, Brazil

Elias Duarte, Federal University of Parana, Brazil
Ahmed Elmisery, Nottingham Trent University, Nottingham, UK
Juan Garcilazo, UADY, Mexico
José Ramón Gállego - Universidad de Zaragoza, Spain
Bachar Hassan, Lebanese University, Lebanon
Djamel Kadraoui, LIST, Luxembourg
Hanna Klaudel, University of Evry, France
Hanan Lutfiyya, University Western Ontario, Canada
Joberto Martins, University of Salvador, Brazil
Claudino Mendes, UNICV, Cape Verde
Jorge Gómez Montalvo, UADY, Mexico
Mirbella Gallareta Negrón, Universidad del Caribe, Mexico
Ismail Guvenc, NC State University, USA
Francisco Moo Mena, UADY, Mexico
Jonice Oliveira, UFRJ, Brazil
Cesar Olavo, IFCE Fortaleza, Brazil
Mauro Oliveira, IFCE Aracaxi, Brazil
Congduc Pham – Université de Pau et des Pays de L'Adour,France
Sergio Rajsbaum, UNAM, Mexico
Rafael Freitas Reale, IFBA, Brazil
Julio César Ramírez Pacheco, Universidad del Caribe, Mexico
Martin Rayrole, Thalesgroup, France
Paulo Nazareno Sampaio, UNIFACS, Brazil
Candy E. Sansores, Universidad del Caribe, Mexico
Sergio Manuel Serra Da Cruz, UFRG, Brazil
Carina Oliveira, IFCE-Aracaxi, Brazil
Omer F. Rana – Cardiff University, UK
Rafael Tolosana, Universidad Zaragoza, Spain
Julio Waissman Vilanova, Universidad de Sonora, Mexico
Marco Winckler, IRIT, University Paul Sabatier, France
Antonio Wendell Rodrigues, IFCE, Brazill

Organisation Committee

Adnan Imeri, LIST Luxembourg and IBISC Laboratory, France
Nazim Agoulmine, IBISC Lab, UEVE-Paris Saclay University, France

Publicity chair

Marcelo Anderson Baptista Dos Santos, IF Sertao-PE, Brazil

Table of Contents

Keynotes

AI at the Edge: Service Orchestration & Enactment Across IoT, Edge & Cloud Resources..............1
Prof. Omer Rana, Cardiff University (UK)

Scalability of LoRa Networks for Dense IoT Deployment Scenarios: limitations and perspectives...2
Prof. Congduc Pham, University of Pau (France)

Long Papers

An Approach of Risk Maturity Models for SOA..3
Rafael Azevedo and Paulo Silva

Smart Cities Evaluations through SMM Framework - Sustainability Maturity Model.....................13
Eber Santana and Éldman Nunes

An Innovative Negotiations and Enactment Smart Contract-based Framework for on-line Sharing Economy Platforms...21
Layth Sliman, Benoit Charroux and Nazim Agoulmine

An Architecture Proposal for E-health Data Collection and Storage Based on Internet of Things and Blockchain...29
Emanuel Coutinho and Alan Nascimento Gomes

Short (Work-in-progress) Papers

BAMSim Simulator...39
Rafael Freitas Reale, Walter Pinto Neto and Joberto S. B. Martins

Task Scheduling Algorithms for Fog paradigm..43
Celestino Barros, Victor Rocio, André Sousa and Hugo Paredes

SDN Controllers - A Comparative Market Survey...48
Francisco Jose Badaro Valente Neto, Constantino Jacob Miguel, Ana Carla dos S. de Jesus and Paulo N.M.Sampaio

Blockchain Applications with Permissionless Distributed Ledger Technology................................52
Emanuel Coutinho and Alan Nascimento Gomes

Keynote 1 - AI at the Edge: Service Orchestration & Enactment Across IoT, Edge & Cloud Resources

Prof. Omer Rana - Cardiff University (UK)

Abstract

Internet of Things (IoT) applications today involve data capture from sensors and devices that are close to the phenomenon being measured, with such data subsequently being transmitted to Cloud data centre for storage, analysis and visualisation. Currently devices used for data capture often differ from those that are used to subsequently carry out analysis on such data. Increasing availability of storage and processing devices closer to the data capture device, perhaps over a one-hop network connection or even directly connected to the IoT device itself, requires more efficient allocation of processing across such edge devices and data centres. Supporting machine learning directly on edge devices also enables support for distributed (federated) learning, enabling user devices to be used directly in the inference or learning process. Scalability in this context needs to consider both cloud resources, data distribution and initial processing on edge resources closer to the user. This talk considers whether a data comms. network can be enhanced using edge resources, and whether a combined use of edge, in-network (in-transit) and cloud data centre resources provide an efficient infrastructure for machine learning and AI.

The following questions are addressed in this talk:

- How do we partition machine learning algorithms across Edge-Network-Cloud resources -- based on constraints such as privacy capacity and resilience?
- Can machine learning algorithms be adapted based on the characteristics of devices on which they are hosted? What does this mean for stability/ convergence vs. performance?
- Do we trade-off accuracy for “explainability” of results? Given a complex parameter space can “approximations” help with explaining the basis of results?

Bio

Omer F. Rana is a Professor of Performance Engineering at Cardiff University, with research interests in high performance distributed computing, data analysis/mining and multi-agent systems. Currently, he is the Dean of International for the Physical Sciences and Engineering College. He previously led the Complex Systems Research Group. He was formerly the deputy director of the Welsh eScience Centre and had the opportunity to interact with a number of computational scientists across Cardiff University and the UK. He serves on the steering committee of Cardiff University's multi-disciplinary "Data Innovation" and "Energy Systems" Research Institutes. Rana has contributed to specification and standardisation activities via the Open Grid Forum and worked as a software developer with London-based Marshall Bio-Technology Limited prior to joining Cardiff University, where he developed specialist software to support biotech instrumentation. He also contributed to public understanding of science, via the Wellcome Trust funded "Science Line", in collaboration with BBC and Channel 4. Rana holds a PhD in "Neural Computing and Parallel Architectures" from Imperial College (London Univ.), an MSc in Microelectronics (Univ. of Southampton) and a BEng in Information Systems Eng. from Imperial College (London Univ.). He serves on the editorial boards (as Associate Editor) of IEEE Transactions on Parallel and Distributed Systems, (formerly) IEEE Transactions on Cloud Computing, IEEE Cloud Computing magazine and ACM Transactions on Internet Technology. He is a founding-member and associate editor of ACM Transactions on Autonomous & Adaptive Systems.

Keynote 2 - Scalability of LoRa Networks for Dense IoT Deployment Scenarios: limitations and perspectives

Prof Congduc Pham - Pau University (France)

Abstract

Recent Low-Power Wide Area Networks (LPWAN) introduced by Sigfox and Semtech are currently gaining incredible interest and are under intense deployment campaigns worldwide. These technologies are mostly simple ALOHA systems with well-known performance limitations. Moreover, due to the extremely low throughput of these long-range technologies, the time-on-air of message can be very large, typically in the range of several seconds, thus dramatically increasing the probability of packet error and collisions. Given the incredible worldwide uptake of LPWAN networks for a large variety of innovative IoT applications, including multimedia sensors, it is important to understand the challenges behind large scale and dense LPWAN deployment, especially because both Sigfox and LoRa networks are currently deployed in unlicensed bands. This talk has a particular focus on LoRa technology as it can be deployed in a private and ad-hoc manner, making community-based deployments possible. In the presention we will review the main LoRa/LoRaWAN characteristics and will then discuss about LoRa/LoRaWAN network scalability in relation with unlicensed band regulations, interferences and various interference mitigation techniques including capture effect, challenges behind channel access mechanism and reliability of Clear Channel Assessment in these LPWAN networks. Perspectives to improve scalability with smarter channel access mechanisms will be discussed.

Bio

Dr Congduc Pham is a Professor of Computer Science at the University of Pau (France). He obtained his Ph.D in Computer Science in 1997 at the LIP6 Laboratory (University Paris 6, Pierre and Marie Curie). His current research interests include wireless sensor networking, Internet of Thing, congestion control/resource allocation and QoS for cloud computing infrastructures. He has published more than 140 papers in international conferences and journals, and gave more than 80 tutorials/keynotes and scientific presentations. In EU H2020 WAZIUP and EU H2020 WAZIHUB, he is one of the scientific expert on Internet-of-Thing and LoRa technology and developed the while LoRa IoT generic framework used in both projects for large-scale deployment of IoT in Africa. He also produced a number of tutorial videos and an online tutorial on sensor technologies, LoRa and IoT kit to be used in hackathons and training sessions. In EU H2020 HUBIQUITOUS he will define the IoT & AI SolutionLab infrastructure to make access to innovative and disruptive technologies more accessible to African startups and entrepreneurs. He will be coordinating the PRIMA-EU INTEL-IRRIS to deploy low-cost and lean solutions for enhancing irrigation efficiency of smallholder farmers.

An Approach of Risk Maturity Models for SOA

Rafael Azevedo[1], Paulo Caetano[1]

[1]Salvador University (UNIFACS), Salvador, Bahia, Brazil.

rafael.azevedo@unifacs.br, paulo.caetano@unifacs.br

Abstract

Intensive use of Service Oriented Architecture (SOA) based technologies provides organizations with more competitiveness and transparency, but incorporates risks and challenges. Although SOA has become the primary means for the delivery and distribution of services and reuse of software components, SOA raises concerns regarding the risks to which the organization is exposed. In order to identify how organizations and academia deal with SOA risks, this paper presents a comparative study of existing risk maturity models, providing support for developing criteria for measuring and analyzing SOA risk maturity once it was not found in the literature specific risk maturity models for SOA. In addition, a literature review is presented in order to identify the state of the art on SOA risk management maturity model proposals. As a result, this paper highlights the need for a risk maturity model for SOA.

1 Introduction

Service Oriented Architecture (SOA) resembles a system with an independent set of cooperating subsystems or services. SOA encompasses the consolidation and reuse of software assets, the reduction of infrastructure complexity and, gradually, the transformation of business processes and Information Technology systems, called IT, into a set of building blocks called service. The demand for services to help build composite applications in a distributed and heterogeneous environment is increasing. The decision to adopt SOA became fundamental for companies looking for competitive market advantages, as explained by [29], through reuse, agility, and adaptability. Web Services are one of the main enablers of SOA and have become an integral part of IT systems and can help to degrade technological barriers and encourage interoperability with business partners, promoting new opportunities for interaction with customers.

With the increasing use of applications dependent on SOA and its prominent role in critical systems of the company, organizations need a comprehensive risk management strategy [29]. Security threats are now more prevalent, and a security breach can cause serious legal, economic, and corporate reputation problems. The risk management and the maturity of risk management in SOA should not be in the background and should be a relevant aspect to by establishing communication between distributed systems. According to [29], for a successful SOA implementation, a risk management and SOA´s maturity analysis must be well defined, planned and executed.

Therefore, due to a lack of knowledge of these impacts, many companies are no longer benefiting from new technologies [9]. This can negatively affect systems development projects, that is, software development without observing practices and methodologies associated with software engineering and risk management, which could bring, with its internalization, benefits, e.g., customer service. delivery time for software projects, increased productivity of development teams, improved quality of software product, cost reduction with systems development, advances in maturity levels, risk mitigation, increased reusability, maintainability, extensibility, reliability, and testability.

In this context, the successful adoption and use of SOA is related to the transfer of IT capabilities to business processes. However, for this transfer to be assertive, it is necessary to monitor and measure the performance improvement of the processes that its services serve [17]. In this sense, the adoption of this architecture must be conducted through governed and measured activities, with the clear purpose of obtaining the maximum return on investments [17].

A relevant factor for the success of risk management is to know how much an organization consistently implements in its risk management process and its degree of maturity, as its efficiency will contribute to meeting the business objectives. Although there are several models that allow an organization to assess their level of risk management maturity, they differ in their application. Some are focused on projects, corporate governance, others on IT governance and SOA governance.

This paper presents a comparative study of existing risk maturity models, providing support for developing criteria for measuring and analyzing SOA risk maturity. In addition, a literature review is presented in order to identify the state of the art on SOA risk management maturity model proposals. As main result, this paper highlights the need for a risk maturity model for SOA.

The remaining sections of this paper are organized as follows. Section 2 describes the basic concepts used for the development of this work, and provides an analysis of the main related works identified in the state of the art. Section 3 presents a comparative analysis of the risk maturity models. Finally, final considerations and suggestions for future work are found in Section 4.

2 Background and Related Works

This section describes the fundamentals of Service Oriented Architecture and brings an overview of related works found in this research field.

2.1 Service Oriented Architecture - SOA

SOA meets the concept of service when it allows a company's business functions to be fully accessible to any of its consumers through IT components. These business functions offer a low coupling and allow total independence from the customer who is accessing the service. According to [11], Service Oriented Architecture is a technological architectural model with different characteristics to support the realization of service orientation and strategic objectives associated with service-oriented computing.

The dimensions of SOA, i.e., people, technologies and processes create artifacts that can support the implementation and use of SOA-based services. Their importance and relevance may vary from company to company, but as a good practice for building SOA solutions, all of these dimensions must be considered in an SOA adoption process, as they can contribute to the elements of risk. Like other strategic initiatives, SOA initiatives also have some considerations that are almost invariant to different business contexts or scenarios, which are these dimensions.

2.2 Related Works

This section discusses the works related to the theme of this article, i.e., the risk management maturity model in SOA. In the bibliographic research carried out, there is a lack of methods, frameworks, or models of IT risk maturity for SOA. However, proposals were identified that brought together some of the most used maturity models in the market to assess the level of capacity and maturity, and good risk management practices.

Table 1 presents a comparison of the related works found in the literature, regarding the application of risk maturity analysis, maturity models, risk maturity models, risk management and use of SOA technology.

WORKS	TYPE OF APPROACH				TECHNOLOGY
	Does it address maturity models?	Does it address risk maturity models?	Do you perform risk maturity analysis?	Does it address risk management ?	SOA
MAZUMDER (2006) [22]	NO	NO	NO	YES	YES
FILIPPOS (2011) [26]	NO	NO	NO	YES	YES
LOWIS (2010) [[20]	NO	NO	NO	YES	YES
COTFAS, et al. (2010) [8]	NO	NO	NO	YES	YES
STEFAN et al. (2008) [27]	NO	NO	NO	YES	YES
HILLSON (1997) [14]	YES	YES	YES	YES	NO
MERYEM AND LAILA (2013) [19]	YES	NO	NO	YES	YES
ARAÚJO AND OLIVEIRA (2012) [2]	YES	YES	NO	YES	NO
MAYER AND FAGUNDES (2008) [21]	YES	NO	YES	YES	NO
RIGON AND WESTPHALL (2011) [25]	YES	NO	YES	YES	NO
CHIN AND COLOMBO (2013) [6]	YES	YES	YES	YES	NO
HARRIS (2013) [13]	YES	NO	NO	NO	YES
JUNIOR, et al. (2012) [18]	YES	NO	NO	NO	YES
GERIĆ (2008) [12]	YES	NO	NO	NO	YES
CIORCIARI AND BLATTNER (2008) [7]	YES	YES	YES	YES	NO
CAMPANÁRIO, et al. (2008) [4]	YES	YES	YES	YES	NO
REN AND YEO (2012) [24]	YES	YES	YES	YES	NO
MAZZAROLO, et al. (2015) [23]	YES	NO	NO	NO	YES
ELMAALLAM AND KRIOUILE (2011) [10]	YES	YES	YES	YES	NO
CARCARY (2013) [5]	YES	YES	YES	YES	NO

Table 1: Comparison of related works

As shown in Table 1, it is possible to verify, through the analysis of the related works, that, although there are works related to SOA, allowing for a greater flexibility of the information systems, none of them covered the aspects related to the risk maturity levels in the SOA dimensions, using risk maturity models. It was also possible to verify that, although there are works that address maturity models and risk maturity models, none approached SOA technology, performing analysis and management of IT risk maturity for SOA.

3 Comparative Analysis of Risk Maturity Models

In order to make a conscious choice of the most appropriate maturity model for the analysis of risk management in SOA, some proposals were selected that will be submitted to a comparative analysis of their characteristics. The following is a brief review of these models.

For the selection of maturity models partially or in its entirety, it was necessary to identify a set of criteria that could be used for this choice, the criteria were grouped in relation to the structure, design, robustness, flexibility, and cost model. The following are criteria that should be considered when selecting the model:

- Number of levels (of the scale) of the maturity model.
- Description of the maturity scales. Names of the maturity levels identified on the scale, so that they are sufficiently clear (self-explanatory).
- Dependence between levels (need or not to fulfill the necessary prerequisites to reach a certain level).
- Domain of application of the model (adherence to the business).
- Evaluation instruments(questionnaires, spreadsheet, etc.) offered by the model.
- Maintaining entity and alignments with reference documents.
- Time of use in the market and traceability of the elements used to reach a level.
- Possibility of comparing the evaluation results (Benchmarking).
- Possibility of customizing the model for application in other domains or adapting it to an organization.
- Training costs and cost with reference material (guides, manuals, standards, etc.).

3.1 Capability Maturity Model Integration - CMMI

The Capability Maturity Model Integration - CMMI is a maturity model for process improvement. Its objective is to assist organizations in improving their product and service development and maintenance processes, through the best practices associated with activities, which cover the product's life cycle from conception to delivery and maintenance. [15].

For progression between maturity levels, CMMI uses a set of specific and generic practices associated with the process areas. To reach a level all the requirements of the previous level must be met.

3.2 Control Objectives for Information and Related Technology - COBIT

According to [16], an association linked to ISACA, which is dedicated to the advancement and international popularization of IT governance and the development and dissemination of COBIT, this is a model and a support tool that allows managers to address deficiencies with respect to the requirements of control, technical issues, and business risks, communicating this level of control to stakeholders.

The COBIT "Plan and Execute" domain consists of ten processes, one of which is the "Assess and Manage IT Risks" process. For the purposes of this work, only the PO9 process - Assess and Manage IT Risks - focus on the proposed maturity study will be considered. The control objectives of PO9 are: PO9.1 Alignment of IT and Business risk management; PO9.2 Establishment of the Risk Context; PO9.3 Event Identification; PO9.4 Risk Assessment; PO9.5 Risk Response; PO9.6 Maintenance and Monitoring of the Risk Action Plan.

3.3 Enterprise Risk Management – ERM

Enterprise Risk Management (ERM) was developed based on the corporate governance precept of the Committee of Sponsoring Organizations - COSO (2004), which determines a model for the identification, assessment, and disclosure of risks that large corporations may be exposed to. The purpose of this model is to provide guidelines for the evolution and improvement of risk management, serving as a basis for the organization to determine whether risk management is being effective, or on the contrary, what it needs to become effective.

The ERM implementation guide developed by the company Protiviti, presents a maturity model to determine the need for improvements in risk management. This model was based on the Software Engineering Institute's CMM model represented by five stages.

3.4 Value Formation in Human Activity Systems - FVSAH

This maturity model proposed by [28] is based on value formation in systems of human activities - FVSAH. The value of institutions has undergone transformations and with that, new concepts, definitions, and ideas have taken the place of physical and human resources in the production of services and products [3]. The FVSAH model has five levels of maturity, with the first level named "functioning" and the last level "reference".

3.5 ISO/IEC 15504

The ABNT NBR ISO/IEC 15504-2 standard defines the structure and conditions for an assessment of organizational maturity based on the assessment of process capacity [1]. The standard describes the requirements for: (i) building maturity models, (ii) conducting organizational maturity assessment and (iii) verifying compliance with organizational maturity assessments.

For the purposes of this work, we will briefly define the subprocess of ISO / IEC 15504 Management Processes, "Risk Management-MAN.4" in order to address issues related to risks.

3.6 Risk Maturity Model – RMM

The Risk Maturity Model - RMM created by [14], suggests four levels of capacity named: Naïve, Novice, Normalized and Natural, which, translating into Portuguese, becomes: naive, participant, normalized and natural. The RMM allows to measure the maturity of the risk from the four areas (Culture, Process, Experience and Application), where the transition between levels occurs from the relationship of the attributes of these areas with the levels.

3.7 Analysis of Maturity Models

After describing the ERM, COBIT, RMM, CMMI, FVSAH and ISO/IEC 15504 maturity models, it is observed that, although the models were created by different entities and with different purposes. In addition, it is possible to identify that some characteristics are common among them, such as: number of maturity levels, dependence between levels, assessment, and measurement instruments.

It is also noticeable that among the models covered, COBIT is the only one to present an assessment tool (non-free), called COBIT Assessment Program, which includes the COBIT PAM (Process

Assessment Model) package where assessments can be performed based on in the descriptions of the maturity level as a whole or with greater rigor based on individual statements in the descriptions of the maturity levels. For the other models, the evaluation instrument can be developed through an evaluation questionnaire, as suggested by Hillson in the RMM model. The COBIT model also offers templates to be used or adapted for application in organizations and has in its structure, a process described for the IT risk management area that is widely used in public and private organizations.

It is also observed that some models have a more complete structure in their architecture than others regarding the approach, treatment, and assessment of risk management, being proposed in its entirety to assess the level of risk maturity, being they the model RMM and ERM.

The RMM model does not offer an assessment tool, suggests the use of an assessment questionnaire but does not exemplify or describe how a questionnaire should be developed.

The importance of CMMI is due to the fact that it is the first maturity model created in Software Engineering, in order to provide two types of representation: continuous and by stages, allowing to focus on a process in isolation and allowing to approach process improvements in stages, called degree of maturity. All other existing maturity models were developed based on CMMI, with levels of maturity in their architecture.

ISO / IEC 31000, in turn, has a clear risk management flow in its structure, but does not address levels of maturity.

The FSVAH maturity model proposes its application in any scope, focusing on the value of risks and human value in the execution and management of activities. This concern with the model and its selection is due to the need to assess the maturity of the SOA dimension "People". As it is a generic model, it is necessary to customize it in relation to the organization's business before its application, which makes the model flexible. It was also noted that the FSAVH model does not provide mechanisms for tracing the evidence used for positioning at a certain level.

ISO/IEC 15504, in turn, is a generic maturity model with a focus on process evaluation. To perform risk management maturity assessment, it is necessary to use it combined with an external model such as the ISO/IEC 31000 standard.

Models Description	ERM	COBIT 4.1	ISO/IEC 15504	CMMI	RMM	FVSAH
Maintainer	COSO	ISACA	ABNT/ISO	SEI	Acadêmico (Hillson)	Acadêmico (Silva)
Num. of Levels	5	6	6	5	4	5
Alignment with other instruments	ISO 31000	ITIL, ISO 17799, PMBOK, PRINCE2, VAL IT, ISO/IEC 15504	ISO 9000, ISO/IEC 2382, ISS/IEC 15288	CMM FOR SW, INCOSE SECAM, EIA 731 SECM	Not applicable	Not applicable
Rastreability	Yes	Yes	Yes	Yes	No	No
Benchmarking	Native	Native	Native	Dependent on external method	Native	Native
Customization	Yes	Yes	Yes	Yes	No	Yes

Training Cost	Yes	Yes	Yes	Yes	Not applicable	Not applicable
Maturity Levels	Level 1: Initial Level 2: Repeatable Level 3: Defined Level 4: Managed Level 5: Optimizing	Level 0: None Level 1: Initial Level 2: Repeatable Level 3: Defined Level 4: Managed and measured Level 5: Optimized	Level 0: Incomplete Level 1: Executed Level 2: Managed Level 3: Established Level 4: Predictable Level 5: In optimization	Level 1: Initial Level 2: Managed Level 3: Defined Level 4: Managed quantitatively Level 5: In optimization	Level 1: Naive Level 2: Beginner Level 3: Normalized Level 4: Natural	Level 1: Operation Level 2: Specialization Level 3: Growth Level 4: Convergence Level 5: Reference
Dependency between Levels	Yes	Yes	Yes	Yes	No	Yes
Measurement	Not addressed	Native	Native	Depends on external method	Native	Native
Domain of the Reference Model	Risk management	IT Control and Management	Generic	Software Engineering	Risk management	Generic
Assessment tools	No	Yes	No	No	No	No
Market Time	11 years	6 years	5 years	7 years	16 years	2 years

Table 2: Comparative table of the main criteria of the maturity models

Table 2 presents comparison key features of maturity models based on criteria defined in the Section 3.

4 Final Considerations

This article aimed to study the risk management maturity models for applicability in the scope of SOA. Sought to investigate the benefits of adoption of risk maturity model for SOA. For this, it made searchable to and review of the literature, in order to get answers to the purposes of this article. A comparative analysis was made of the main governance maturity models in SOA and a review of proposals for risk management maturity models for SOA. Identified that there is no maturity model in the market and academic that meets the main criteria considered in this work (Section 3) for maturity models in risk management in SOA, therefore, it is evident the need to develop a risk maturity model specific to service-oriented architecture.

From this work can be concluded that the right choice of the maturity model for managing risks in SOA brings benefits to: Corporate Governance, Governance of IT Governance SOA, auditors, to development teams and software for companies' development of SOA solutions, allowing a holistic view of the level of risk maturity in SOA in its dimensions.

As future work, the next steps are: (i) development of an instrument or method for assessing the level of risk maturity in SOA; (ii) creation of a risk maturity model for SOA, elaborated based on the studies and comparison of the risk maturity models presented in this work; and (iii) evaluation of the proposed model through a practical application in one or more organizations that have a service-oriented architecture as a software development model.

Acknowledgments

I would like to extend my special thanks to Professor Dr. André Araújo from Federal University of Alagoas for the great support and contribution in this paper.

References

[1] ABNT. (2008b). ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO 73: Primeira Edição. Gestão de Riscos — Vocabulário. Rio de Janeiro: ABNT.

[2] ARAUJO, M. S. (2012). Estudo comparativo de modelos de maturidade aplicados à gestão de riscos - uma abordagem sob a perspectiva da tecnologia da informação. Acesso em 05 de Apr de 2019, disponível em http://www.excelenciaemgestao.org/Portals/2/documents/cneg10/anais/T14_0191.pdf

[3] BOLTOUN, R. E., LIBERTY, B. D., & M., S. S. (2000). *Cracking the Value Code: How success businesses are creating wealth in the New Economy.* New York.

[4] CAMPANÁRIO, M. d. (2012). Metodologia e Níveis de Maturidade em Gestão de Riscos de Projetos nas empresas de Serviços de Telecomunicações. *CONVIBRA - Congresso Virtual Brasileiro de Administração*. Acesso em 22 de May de 2019, disponível em http://www.convibra.com.br/artigo.asp?ev=25&id=1807

[5] CARCARY, M. (2013). IT Risk Management: a capability maturity model perspective. *Innovation Value Institute, National University of Ireland Maynooth*. Acesso em 11 de May de 2019, disponível em www.ejise.com/issue/download.html?idArticle=858

[6] CHIN, H. Y. (2013). Boas práticas de gestão de risco corporativo: estudo de dez empresas. Acesso em 06 de Apr de 2019, disponível em http://www2.pucpr.br/reol/index.php/rebrae?dd99=pdf&dd1=7664>. Acesso em 06 abr

[7] CIORCIARI, M. B. (2008). Enterprise Risk Management Maturity-Level Assessment Tool. *Society of Actuaries*. Acesso em 22 de May de 2019, disponível em http://jvvnz.x.incapdns.net/library/monographs/other-monographs/2008/april/mono-2008-m-as08-1-ciorciari.pdf

[8] COTFAS Liviu, P. D. (2010). Techniques for Service Oriented Architecture Applications. Acesso em 09 de Jul de 2019

[9] DEBRECENY, R. (2009). Research on IT governance, risk, and value: Challenges and opportunities. *Journal of Information Systems 27 (1)*, 129-135.

[10] ELMAALLAM, M. K. (2011). Towards a Model of Maturity for IS Risk Management. *International Journal of Computer Science & Information Technology (IJCSIT), 3*(4). Acesso em 09 de May de 2019, disponível em http://airccse.org/journal/jcsit/0811csit14.pdf

[11] ERL, T. (2009). *Service-Oriented Architecture (SOA): Concepts, Technology, and Design.* (9^{a} Edition ed.). Prentice Hall.

[12] GERIĆ, S. (2008). Service-Oriented Architectures Maturity Models. Acesso em 03 de Mar de 2019, disponível em https://www.mtf.stuba.sk/docs/internetovy_casopis/2008/4mimorc/geric.pdf

[13] HARRIS, T. (2013). A SOA Maturity Model. *A SOA Maturity Model.* . Acesso em 12 de Apr de 2019, disponível em http://www.thbs.com/knowledge-zone/soa-maturity-model

[14] HILLSON, D. (1997). *Towards A Risk Maturity Model.* Acesso em 19 de Jun de 2019, disponível em http://www.risk-doctor.com/pdf-files/rmm-mar97.pdf

[15] INSTITUTE., S. –S. (November de 2010). CMMI for Services. Pittsburgh, PA. Carnegie Mellon.

[16] ITGI. (2019). *ISACA.* Retrieved Apr 15, 2019, from ISACA: http://www.isaca.org/cobit/pages/default.aspx

[17] JANIESCH, C. K., & ROSEMANN, M. (2009, December 4). Conceptualisation and Facilitation of SOA Governance. *In: Proceedings of ACIS 2009: 20th Australasian Conference on Information Systems*.

[18] JUNIOR, J. J. (2012). Pontos chaves para adoção de uma arquitetura orientada a serviços: uma análise comparativa de modelos de maturidade SOA da indústria. Acesso em 27 de May de 2019, disponível em http://www.lbd.dcc.ufmg.br/bdbcomp/servlet/Trabalho?id=11327

[19] KASSOU, M. K. (2013). A Goal Question Metric Approach for Evaluating Security in a Service Oriented Architecture Context. *IEEE, Europa. 2013.* Acesso em 07 de May de 2019, disponível em http://arxiv.org/ftp/arxiv/papers/1304/1304.0589.pdf

[20] LOWIS, L. (2010). Towards automated risk identification in Service-Oriented Architectures. Acesso em 08 de May de 2019, disponível em http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.143.6303&rep=rep1&type=pdf

[21] MAYER, J. F. (2008). Proposta de um modelo para avaliar o nível de maturidade do processo de gestão de riscos em segurança da informação. Acesso em 15 de May de 2019, disponível em http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st02_03_wticg.pdf

[22] MAZUMDER, S. (2006). A Perspective on Implementation Risks. *SETLabs Briefings*. Retrieved Jun 08, 2019, from https://s3.amazonaws.com/academia.edu.documents/44814562/soa-perspective-implementation-risks.pdf?response-content-disposition=inline%3B%20filename%3DSOA_A_Perspective_on_Implementation_Risk.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYY

[23] MAZZAROLO, C. F. (2015). A Method for SOA Maturity Assessment and Improvement. Acesso em 21 de May de 2019, disponível em http://www.ewh.ieee.org/reg/9/etrans/ieee/issues/vol13/vol13issue1Jan.2015/13TLA1_30Mazzarolo.pdf

[24] REN, Y. T. (2012). Risk Management Capability Maturity Model for Complex Product Systems (Cops) Projects. *Center for Project Management Advancement (CPMA), School of Mechanical and Production Engineering, Nanyang Technological University, Singapore*. Acesso em 21 de May de 2019, disponível em http://www-scf.usc.edu/~yingtaor/publications/RM_CMM_SysEng.pd

[25] RIGON, E. A. (2011). Modelo de avaliação da maturidade da segurança da informação. Acesso em 20 de Apr de 2019, disponível em http://www.lbd.dcc.ufmg.br/colecoes/sbsi/2011/modelodeavalicao.pdf

[26] SANTAS, F. (Set de 2011). Mitigating Service-orientation Risk With RUP. *Service Technology Magazine, n. 54*. Acesso em 07 de May de 2019, disponível em http://www.servicetechmag.com/system/application/views/I54/0911-2.pdf

[27] SHULTE, S. R. (2008). Potential Risks and Benefits of Service-Oriented Collaboration: Basic Considerations and Results from an Empirical Study. *In: International Conference on Digital Ecosystems and Technologies – IEEE, 2008, Proceedings. Europa: IEEE, 2008.* Acesso em 31 de Mar de 2019, disponível em ftp://ftp.kom.tu-darmstadt.de/papers/SRE+08.pdf?

[28] SILVA, J. M. (2012). *Apostila de Formação de valor em Sistemas de Atividades Humanas. Faculdade de Tecnologia, Núcleo de Engenharia de Produção, UnB.* Brasilia.

[29] TIPNIS, A., & LOMELLI, I. (2009). Security – A Major Imperative for a Service-Oriented Architecture. HP. Retrieved Mar 19, 2019, from http://docplayer.net/6863478-Security-a-major-imperative-for-an-service-oriented-architecture.html

Smart Cities Evaluations through SMM Framework - Sustainability Maturity Model

Eber da Silva de Santana[1,21] e Éldman de Oliveira Nunes[12]
[2] Universidade Salvador - PPGCOMP of Salvador, Bahia, Brazil
eberss@gmail.com, eldman.nunes@unifacs.br

Abstract

The insertion of Communication and Information Technologies (ICT's) in the scope of city management can facilitate managers' decision making, thus creating improvements in the infrastructure and services offered to citizens and can serve as a subsidy to the creation of Intelligent Cities. To assess the level of maturity of an intelligent city, this article aims to propose and apply a new framework, because most of the models used do not follow a standard and/or are not able to be compared with each other. Named SMM - Sustainability Maturity Model, it was inspired by the CMMI maturity indexes, the COBIT process controls, and used ISO 37122 indicators, thus serving as statistical measurement of ISO indicators, adapted to the CMMI maturity model and COBIT best management practices. In this way, the stages of the framework were developed, and a case study was conducted in the cities of São Paulo, Rio de Janeiro, and Salvador to validate it. As a result, it was observed that the SMM allowed classifying the cities by their level of maturity. Such measurement and comparison of maturity level were considered for the Intelligent Economy Domain of 3 of the 4 largest Brazilian cities in population. This evaluation adds value to the city that wishes to become intelligent, thus being able to serve as a basis for the application of new evaluations and measurement of the evolution of these environments.

Keywords— Smart Cities, SMM, Maturity, ISO 37122, CMMI, COBIT

1 Introduction

Definitions of Smart Cities may vary from one author to another. One of them states they are communities that seek to transform life and work effectively using Information Technology. Managers from various locations around the world claim that their cities are smart just because they have ICT-based initiatives, which is not correct (GIFFINGER et al., 2007).

With the emergence of the concept of smart cities, several indexes and indicators were created to measure the potential of cities, as well as neighborhoods and small towns, to develop maturity models to classify these locations. The term "smart city" is not used uniformly, ranging from cities with high ICT use to cities whose education or intelligence of their inhabitants is recognized (WEISS, 2016).

Smart cities can build innovative solutions for urban centers. They identify the priority characteristics of management by local government to find ways to increase the potential and solutions to the problems of the population (LEMOS, 2016).

These cities can use their resources, solving the demands of their inhabitants without wasting money, and with high creative potential. Thus, innovations in the management of municipal governments can be a differential in Public Administration intelligently and assertively, allowing to face problems faced by the population (WEISS, 2016).

[1] Eber da Silva de Santana
[2] Éldman de Oliveira Nunes

Several standards and/or models have been developed that provide a set of indicators as a recommendation of what to measure and how it should be measured. However, the standards do not define a standardized metric to measure at what level of maturity cities intend to become smart (GAMA, ALVARO, and PEIXOTO, 2012).

In this sense, this research aims to verify the applicability of the Sustainability Maturity Model (SMM), developed by Santana et al. (2019).

The SMM model was developed to propose a framework to evaluate the degree of maturity of an Intelligent City. The maturity models that served as inspiration for the development of SMM were the Capability Maturity Model (CMMI), together with the management of COBIT, added to the ISO 37122 standards (SANTANA et al., 2019).

This research is justified by the attempt to evaluate the applicability of SMM in metropolises such as Salvador, Rio de Janeiro, and São Paulo, observing the degree of maturity and confronting it with what is disclosed by their respective managers. The relevance of this study rests in an attempt to contribute to filling the existing gap in a standardized evaluation of a Smart City.

This article is organized into five sections, being in this first one presented the objective of the work and its relevance. In the 2nd section, the theoretical reference is presented, giving theoretical support to the research. The 3rd section presents the methodological path used to achieve the proposed objective. In the 4th section, the analysis of the results found is presented. Finally, in the 5th and last section, the conclusion and/or final considerations are presented, as well as suggestions for future research.

2. Background

From the concept emergence of smart cities, several indexes, indicators, and measurement models were created to evaluate them (SANTANA; NUNES; SANTOS, 2018). Researchers proposed their models based on the indicators and/or domains they found most relevant for a smart city. Some of these models have levels that serve to measure, analyze, and graduate the level of intelligence of a city (SANTANA et al., 2019). The models found do not always apply in the same way to more than one location, since each region has its specific characteristics and these do not contemplate them in their entirety (JUNKES, 2016).

Faced with this context, there is a wide variety of classification indicators, as there are various perspectives on how cities can be classified, seen, and evaluated by different social actors. However, most of the models used do not follow a pattern and are not comparable over time and with each other (GUIMARÃES, 2018). To illustrate the gap existing in the evaluation of Smart Cities, Box 01 presents the models found in research and their respective limitations.

Model	Models' limitations
Giffinger et al. (2007)	First to be carried out with Smart Cities focused on medium-sized cities and stereotyped as ranking.
SCMM (Smart City Maturity Model)	The strength of this model is the gradual evolution and readiness of technology. Limited understanding of the model and its simplicity are pointed out as limitations.
BR-SCMM (Brazilian Model)	Applicable in a more interesting way to cities that are starting the development process to become smart. Limitation: the need for data, simplicity, and the fact that the model is still under development.
WCCD Certification Model	It is based on a universal standard (ISO), allowing comparison between cities already certified. The model's limitation is the complex and restricted data collection and the complexity of the analysis.
MMT Model (Technological Maturity)	As a strong point, it has a maturity scale of five levels. As a limitation, it is based on only three facts, being people, business, and technology; the model is still in development.
IDC Model(GOVER)	As a relevant point of this model is the gradual evolution between the five levels and, as a limitation, it is still in development.
SC4A Model (SMART CITY FOR ALL)	A positive point in this model is identified as the gradual five-level scale, the focus on accessibility and inclusion of information technology, and the fact that the model is still under development.
Modelo RCSC (Ranking Connected Smart City)	The strong point of this model is the existence of annual awards for cities that are positively evaluated by it, in addition to the gradual and quantitative analysis. As a limitation, we have complex evaluation and applicability.
Modelo ESC (European Smart Cities)	In this model, the positive point is the possibility of obtaining indicators on top of the 27 applicability domains, and as a limitation, its complex applicability, being able to make the comparison of up to three cities.

Modelo SCIP (Smart City Index Portugal)	Five positive points of this model stand out: the comparison of performance between municipalities; having five domains; using scale variation from 0 to 10; revealing the cities with the most inherent characteristics of a smart city and having a global comparative analysis. Limitation: the fact that it is still under development.
RBCIH Model (Brazilian Network of Intelligent and Human Cities)	This model is based on the possibility of exchanging experience between cities, this being a positive point, besides aiming to create a seal for classifying a smart city. As a limitation, it uses the indicators of ISO 37120, which are not suitable for smart cities.
NBR ISO 37120 Model	The standard has several strong points, highlighting the fact that it is an international standard that serves as a reference for standardization and normalization. As a negative point, this standard is not specifically designed for smart cities.
ISO 37122 Model (Indicators for Smart Cities)	ISO 37122 will help cities implement Smart Cities policies to provide better services to citizens.
WEISS Model (Readiness Assessment Model)	This model is focused exclusively on ICT perspectives. The fact that its applicability is complex stands out as a limitation.
IBMCCI Model	In the development of this model little would be added, since several authors have already formulated their classification and evaluation models.

Table 1: Smart City Assessment Models

3 Methods

Due to the need to establish a standard model to measure the level of intelligence for cities that have different characteristics and are at different points of maturity, Santana et al., (2019) proposed the SMM framework - Sustainability Maturity Model. According to the authors, SMM was inspired for its development by CMMI (PAULK, 1993), together with the management of COBIT (ISACA, 2012), added to the ISO 37122 standards (SANTANA; NUNES; SANTOS, 2018).

According to Paulk (1993), the CMMI model is a forerunner when it comes to maturity, linked to maturity levels and processes and thus serving as a reference for other models. The COBIT, developed by Information Systems Audit and Control Association (ISACA), has as main objective to generate value for the managerial processes of an organization (ISACA, 2012). ISO 37122 - Indicators for Smart Cities, is the first standard of the agency directed exclusively to Smart Cities. Cities adopting ISO 37122 will have standardized definitions and methodologies for a set of key performance indicators as tools to become more sustainable and smart. With ISO 37122, the indicators informed in the standard were used, which in total include 75, which are indicated for smart cities. ISO 37122 is divided into 19 thematic areas and uses 6 domains: Smart Economy, Smart People, Smart Governance, Smart Mobility, Smart Environment, and Smart Life (ISO, 2017).

The SMM Framework is composed of 5 stages, as can be seen in Figure 1. This way, it is necessary to collect data from the external environment, passing through the application of ISO 37122 through the Maturity Test, data analysis, identification of the maturity level of the city inspired by CMMI, until reaching the process analysis of the information obtained inspired by COBIT, and/or the archiving of the whole process in a database for further consultation, comparability, and knowledge of those interested. Each step will be described as follows.

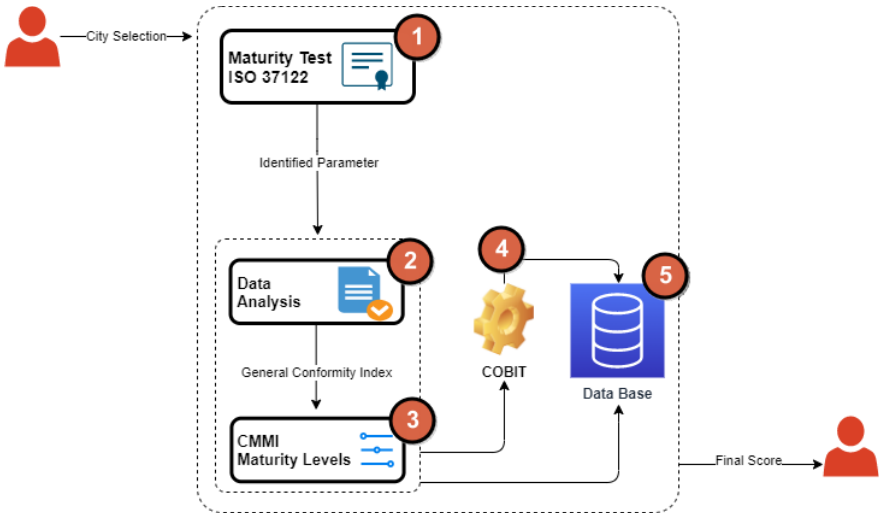


Figure 1: SMM - Sustainability Maturity Model Framing

Maturity Test:

Step 1 consists of applying the Maturity Test, formulated based on ISO 37122 and CMMI, and consisting of three steps: 1) choose the domains or subdomains to be evaluated; 2) calculate, based on ISO 37122, the indicators of the selected domains; 3) verify the scale of parameter evaluation of each indicator, developed from the level of the degree of maturity, based on the CMMI, in which it is possible to identify if the indicator was fully met (AT - Fully Met), partially met (AP - Partially Met), or not met (NA - Not Met).

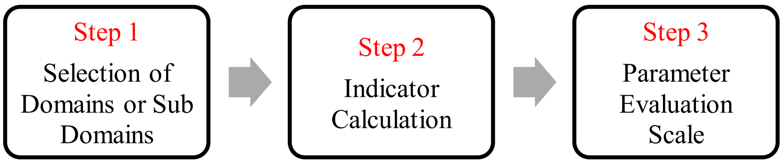

Step 1
Selection of Domains or Sub Domains
Step 2
Indicator Calculation
Step 3
Parameter Evaluation Scale

Figure 2: Step processes

Data Analysis:

The second step consists of the Data Analysis, supported by the equations proposed in Table 2. After selecting and obtaining the indexes of the domains, the components that will define the classification index of smart cities, one reaches a point of formulation of the SMM that implies an aggregation of the calculated indexes for each dimension, consisting of the analysis of data. For the validation phase, of the data complying with what is determined by ISO 37122 for the calculation of each indicator, the data collection strategy was used in the main open public data media, the data were collected from various databases made available by public bodies and organizations, municipalities of national industrial property institutes, regulatory agencies, national telecommunications agency, among others.

The indexes are extremely important tools for improving communication, as they seek to simplify the information on complex phenomena so that its understanding is clear to all types of audiences and thus can guide decision making.

Often the composition of the index can give different weights for its components, which can be questioned as subjectivity since depending on the weights assigned to each component, the result of the index can vary a lot.

1. General Compliance Index (ICG) - **Equation (1)**	
$$ICG = \frac{\sum_{k=1}^{p} ICD_k \times PD_k}{\sum_{k=1}^{p} PD_k}$$	The General Conformity Index (ICG) is the index that will indicate the level of maturity that the city is in the global aspect, since for its calculation it involves all indicators. It is the weighted average multiplying the ICD (Domain Compliance Index) by the PD (Domain Weight) divided by the sum of the PD, where k = 1, 2, 3 ... p where p is the total of Domains. Ranging from 0 to 100%, its formula is defined by equation (1).
2 - PD = DOMAIN WEIGHT - **Equation (2)**	
$$PD = \sum_{j=1}^{m} PSD_m$$	Where PD (Weight of Domains) is the sum of PSD (Weight of Sub-domains) represented by equation (2).
3. Domain Compliance Index (ICD) - **Equation (3)**	
$$ICD = \frac{\sum_{j=1}^{m} IMSD_j \times PSD_j}{\sum_{j=1}^{m} PSD_j}$$	The Domain Conformity Index (ICD) is the index that will indicate the level of maturity that the city is in the domain selected for analysis, for its calculation the indicators of the specific domain are selected. It is a weighted average which is calculated by multiplying the IMSD (Subdomain Maturity Index) by the PSD (Subdomain Weight) divided by the sum of the PSD having j = 1, 2, 3 ... m, being the total subdomains, varying 0 to 100% and its formula is defined by equation (3).
4. Sub-domain Maturity Index (IMSD) - **Equation (4)**	
$$IMSD = \frac{\sum_{i=1}^{n} EAP_i \times RI_i}{TTI \times EAP[TA]}$$	The Subdomain Maturity Index (IMSD) is the index that will indicate the level of maturity that the city is in the subdomain selected for analysis, for its calculation the indicators of the specific subdomain are selected. It is the sum of the product between the EAP and IR, where EAP is the Scale of the Parameter Evaluation (0 = NA (Not Answered), 1 = PA (Partly Answered) and 2 = TA (Fully Answered)) and IR is the Result

	of Indicators, divided by the TTI (Total ISO Indicators in the Subdomain) multiplied by the EAP [TA] (Fully Answered Scale of the Parameter Evaluation) having i = 1, 2, 3 ... n, being the total of indicators of each subdomain . Defined by equation (4).

Table 2: Equations developed for Step 2

Maturity Level Assessment:

Step 3 consists of directing the processes, making the result meet the needs and expectations of the areas through planning, and monitoring the results obtained in step 1. It is in this stage that it is possible, through the maturity levels inspired by CMMI, to evaluate at which level the city is, within a scale that varies from 1 to 5, according to Chart 3.

LEVEL	DETAILS
1- Initial (Not Reached) (0 to 15%)	At this level, the cities begin. This phase indicates that cities plan and shape the information systems they will use to integrate their smart solutions.
2- Managed (Partially Reached) (>15% to 50%)	At this level, cities are called efficient, seeking innovation and pioneering in information technology solutions, with a greater focus on supporting decision-making for both citizens and governments, through the use of data obtained in various fields.
3- Defined (Largely achieved) (>50 to 85%)	At this level, data are already collected and accessible to the population through properly functioning information systems, and cloud computing systems are used, integrated as services, and available to both citizens and third parties.
4- Quantitatively Managed (Fully Achieved) (> 85 to 100%)	At this level, cities are in a stage of integrated resources and available in the form of services for both citizens and applications. At this stage, the use of computing aims to be available everywhere.
5- In Optimization (Optimized) (100%)	At this level, cities are classified as perfected, with applied innovations and becoming pioneers in technological solutions.

Table 3: Level of maturity inspired by CMMI

Analysis of results and data storage:

The fourth stage consists in the analysis of the results obtained so far through the application of COBIT because after identifying the level of maturity that the city is, it is possible to have two paths: 1) the city is below level 5, in which case the COBIT processes should be used to analyze the points that need to be improved and perform an intervention; 2) the city is already at level 5: In this case, it is possible to jump to Stage 5, already for the data storage, or still go through Stage 4, where it will be possible to review the processes keeping the continuous improvement and still seeing in which points the city can still be optimized. Stage 5 consists of the data storage, through a database, also developed for this purpose.

4. Results and Discussions

The proposed framework, SMM, aims to suggest a standardization for measuring the level of intelligence of a city. The intention is that it should be a universal model, thus being able to be applied to any city with any characteristics. The indicators of each theme are classified among general indicators, which are considered essential for the analysis of the performance of smart cities.

In this case, it was held in three large Brazilian cities, Salvador, Rio de Janeiro, and São Paulo, based on publicly available data. The data used were obtained through electronic platforms such as municipal websites and IBGE, to validate the proposed framework. It is a cross-sectional study since it was carried out in a certain instant of time, applied based on data from the year 2018.

In this article, the Intelligent Economy Domain was selected to validate SMM because it refers to the economic situation and the actions taken by a country to increase its wealth or reduce poverty and development among the 6 main existing domains that contemplate economy, people, governance, mobility, environment, and quality of intelligent life, which are at the root of the formulation of any concept of smart cities, according to Giffinger et al.

The first calculated economy domain indicator refers to the percentage of local companies hired to provide municipal services that have openly available data communication, as data communication meaning the process of using computing and communication technologies to transfer data from one place to another and vice versa.

The second indicator aims to calculate the annual number of new startups per 100,000 inhabitants. The third indicator of the Economy sub-domain seeks to calculate the percentage of labor employed in the ICT sector. The fourth and final indicator of this sub-domain seeks to identify the percentage of the labor force employed in the Education and Research and Development sectors per capita per year.

For the Finance sub-domain, the first indicator to be calculated is the percentage of the municipal budget spent on innovations and smart city initiatives per year. Smart city innovations and initiatives are helping to pave the way for more livable and sustainable cities. The second index to be calculated from this sub-domain is the annual amount of tax charged from the sharing economy as a percentage of total tax charged. Finally, the third and final indicator of the Finance sub-domain is the percentage of payments to the city that are paid electronically based on electronic invoices.

In Table 4 it is possible to visualize the results obtained with the calculation of each index of the subdomains Economy and Finance, for each city analyzed (Salvador, Rio de Janeiro, and São Paulo).

CITIES	**ECONOMY**				**FINANCE**		
	1º sub	**2º sub**	**3º sub**	**4º sub**	**1º sub**	**2º sub**	**3º sub**
Salvador	4,77%	2,53%	4,51%	20,60%	7,75%	27,53%	21,25%
Rio de Janeiro	49,75%	8,38%	10,80%	21,00%	19,75%	26,78%	30,55%
São Paulo	62,76%	37,52%	36,80%	17,28%	30,00%	29,64%	37,62%

***Table 4:** Results of Economy and Finance Subdomains.*

Once the selected Domain, Intelligent Economy, has been calculated, the third stage of the Maturity Test is started, which is to fill in the Parameter Evaluation Scale according to Table 5, where it is possible to identify if the indicator has been fully met (TA - Fully Met), being in the range of 85.1% - 100%, partially attended (PA - Partially attended), being in the range of 15.1% - 85%, or not attended (NA - Not attended), being in the range of 0 - 15%, which will subsidize the next stage of the SMM of the analysis of the weights of the domains.

Maturity Test Questions for the Smart Economy Domain	**SALVADOR**			**RIO DE JANEIRO**			**SÃO PAULO**		
	NA	**PA**	**TA**	**NA**	**PA**	**TA**	**NA**	**PA**	**TA**
	0	**1**	**2**	**0**	**1**	**2**	**0**	**1**	**2**
1 What percentage of local companies are hired to provide municipal services with openly available communication data?	**X**				**X**			**X**	
2 What is the annual number of new startups per 100,000 inhabitants?	**X**			**X**				**X**	
3 What is the percentage of the workforce employed in the Information and Communication Technology (ICT) sector?	**X**			**X**				**X**	
4 What is the percentage of the workforce employed in the Education, Research, and Development sectors?		**X**			**X**			**X**	
Total per Subdomain	**3**	**1**	**0**	**2**	**2**	**0**	**0**	**4**	**0**
5 What percentage of the municipal budget is spent on innovation and smart city initiatives per year?	**X**				**X**			**X**	
6 What is the annual amount of tax collected from the total collected?		**X**			**X**			**X**	
7 What percentage of payments to the city are paid electronically based on electronic invoices?		**X**			**X**			**X**	
Total per Subdomain	**1**	**2**	**0**	**0**	**3**	**0**	**0**	**3**	**0**

***Table 5:** Scale result of parameter evaluation – Salvador, Rio de Janeiro e São Paulo*

After finishing Step 1, where the Maturity Test was performed in each Municipality, finding the Evaluation Parameters of each Indicator, the application of the proposed equations (1, 2, 3 and 4) is performed, thus identifying the ICD, IMSD - Economy, and IMSD - Finance indexes, according to Table 6.

INDEX	**Salvador**	**Rio de Janeiro**	**São Paulo**
ICD	29,20%	45,00%	47,50%
IMSD – Economy	12,50%	25,00%	48,50%

IMSD - Finanças	33,33%	47,00%	49,50%

Table 6: *Index Results*

In the Smart Economy Domain, regarding the city of Salvador, a Domain Compliance Index (DCI) was identified from equation (3), amounting to 29.20%, as shown in Table 6. A Maturity Index by Subdomain was also obtained from equation (4), with a value of 12.50% for the Subdomain Economy, while for the Subdomain Finance, the value was 33.33%. Since we are dealing with only one Domain, the General Compliance Index (GCI), equation (1), will not be calculated, which is relevant to be observed when analyzing all Domains together.

In the City of Rio de Janeiro, a Domain Compliance Index (DCI) was found from equation (3), in the value of 45%, as presented in Chart 6. A Maturity Index by Subdomain was also obtained from equation (4), worth 25% for the Subdomain Economy, while the Subdomain Finance was found to be 50%. As in the municipality of Salvador, since we are dealing with only one Domain, the General Compliance Index (GCI), equation (1), which is relevant to be observed when analyzing all Domains together, will not be calculated.

In the City of São Paulo, a Domain Compliance Index (DCI) was found from equation (3), in the value of 47.50%, as presented in Chart 6. A Maturity Index by Subdomain was also obtained from equation (4), with a value of 48.50% for the Subdomain Economy, while for the Subdomain Finance, with a value of 49.50%.

From the result, it was possible to identify the degree of maturity of each Domain and Sub-Domain for Salvador, Rio de Janeiro, and São Paulo. Table 7 shows the Maturity levels per Domain and Sub-Domain of each analyzed Municipality.

INDEX	**Maturity Level**					
	Salvador		**Rio de Janeiro**		**São Paulo**	
ICD	29,20%	2 - Managed	45,00%	2 – Managed	47,50%	2 - Managed
IMSD – Economy	12,50%	1 - Not Reached	25,00%	2 – Managed	48,50%	2 - Managed
IMSD - Finance	33,33%	2 - Managed	47,00%	2 – Managed	49,50%	2 - Managed

Table *7 – Maturity Level*

Thus, it is possible to observe that the cities analyzed in this study are at a level that needs development in the chosen Domain. It is observed that both the city of Rio de Janeiro and São Paulo have ICD - equation (3) - and IMSD - equation (4) -, for Economy and Finance at the Managed Level, level 2, which corresponds to a percentage between >15% and 50%, being considered partially reached.

This is the stage where cities are called efficient, seeking innovation and pioneering in information technology solutions, with a greater focus on supporting decision-making for both citizens and governments, using data obtained in various fields.

In Salvador, the city also has ICD, equation (3), and IMSD- Finance, equation (4), in the Managed Level, but its IMSD - Economy, equation (4), is in level 1, Initial - Not Reached In this level 1 is the phase where the cities begin. This phase indicates that cities plan and shape the information systems they will use to integrate their intelligent solutions.

Thus, the manager must search from the Compliance Index (DCI) by Domain and the IMSD (Sub-domain Maturity Index) to verify what measures must be taken to reach level 5 of maturity, having the four domains as direction and maintenance. It is worth mentioning that the improvement of the domains can be evaluated individually or collectively to obtain the maximum level for the city. This phase is important because it allows achieving success and, consequently, improvement in the quality of services (BALBO; VENDRAMEL; TOLEDO, 2014).

With this analysis the actors can identify the strengths and weaknesses of the city for which they are responsible, thus facilitating the implementation of measures that improve performance or even serve as a reference and inspiration for other cities that want to become smart if they are at an "In Optimization" level. Thus, with the result of the Test, it is analyzed in which degree of maturity the city is based on the 5 levels of maturity.

5. Final Considerations

This article proposed the development of the SMM framework for smart city maturity analysis, based on ISO 37122 and inspired by the CMMI maturity model, as well as using COBIT processes. From the application of SMM stages in the cities of Salvador, Rio de Janeiro, and São Paulo, it was possible to identify that the economic domain of the cities is at the initial level of maturity, thus allowing managers to analyze and take measures to reach higher levels, as well as the data that were collected, serving for comparability with other cities that use SMM. The proposed framework is a useful tool for any city, regardless of its size, type, origins, and characteristics, since it also allows the study of each domain separately and, over time, the monitoring of its evolution. According to the established objective and proposal, SMM has proved to be a relevant tool for the analysis and evaluation of a smart city, being possible, from its domains and indicators, to identify the level of maturity of the city to be analyzed. In the absence of a diagnosis, the actions may become disoriented, poorly prioritized, and redundant, not offering the expected return. Thus, the application of SMM makes it possible to verify the diagnosis by domains, thus observing in which aspect the city under study stood out, as well as its lags.

It is observed that the proposed objectives have been achieved and the results show that the model can serve as a basis for application in the evaluation and measurement of smart cities. As contributions of future work, it is suggested the insertion of new modules to the SMM framework, as well as the use of artificial intelligence techniques to consolidate the General Compliance Index and its application in other municipalities.

References

BALBO, A. P.; VENDRAMEL, W.; TOLEDO, M. B. F. Software Measurement at CMMI and MPS.BR. 2014. Devmedia.

GAMA, K .; ALVARO, A., PEIXOTO, E. “Towards a Technological Maturity Model for Smart Cities.” In: VIII Brazilian Symposium on Information Systems - SBSI, 2012, São Paulo, SP. Proceedings ... (online). São Paulo: SBSI, 2012. Available at <http://roitier.pro.br/wp-content/uploads/2017/09/0018-2.pdf&gt; Accessed on June 26 2020.

GIFFINGER, R. et al. Smart cities. Ranking of European medium-sized cities, Final Report, Centre of Regional Science. Vienna: UT, 2007.

GUIMARÃES, José Geraldo de Araújo. Smart cities: proposal for a Brazilian model for multi ranking classification. 2018. 278 f. Thesis (Doctorate in Administration) - University of São Paulo - USP, São Paulo, 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. ISO 37122. Sustainable development in communities - Indicators for Smart Cities. 2017. International Organization for Standardization.
ISACA. IT Governance Institute, COBIT 5. Available at: http://www.isaca.org

ISO. ISO 37122 Sustainable development in communities - Indicators for Smart Cities. 2017. International Organization for Standardization. Available at: <https://www.iso.org/obp/ui/#iso:std:iso:37122:dis:ed-1:v1:en>. Accessed on: 27 out. 2020.

JUNKES, Darlan. How to Measure Smart Cities? 2017. Available at: <http://via.ufsc.br/como-mensurar-cidades-inteligentes/>. Accessed on: 04 jun. 2020.

LEMOS, André. Smart cities: How can new technologies - such as cloud computing, big data and the Internet of Things - improve living conditions in urban spaces? 2013. Available at: <https://rae.fgv.br/sites/rae.fgv.br/files/artigos/gv_v12n2_46-49.pdf>. Accessed on: 12 nov. 2020.

PAULK, M. C. et al. The Capability Maturity Model for Software. 1993. Available at: http://sunnyday.mit.edu/16.355/cmm.pdf. Accessed on: 20 dez. 2018.

SANTANA, E. S .; NUNES, E. O .; PASSOS, D. C .; SANTOS, L. B. SMM: A Maturity Model of Smart Cities Based on Sustainability Indicators of the ISO 37122. International Journal of Advanced Engineering Research and Science, v. 6, n. 2, p.013-020, 2019. AI Publications. http: //dx.doi: 10.22161 / ijaers.6.2.2.

WEISS, M. C. Smart Cities: proposing an assessment model for the readiness of information and communication technologies applicable to city management. 2016. Thesis (Doctorate) - Centro Universitário FEI, São Paulo, Brazil.

An Innovative Negotiations and Enactment Smart Contract-based Framework for on-line Sharing Economy Platforms

Layth Sliman[1][2], Benoit Charroux[1], and Nazim Agoulmine[2]

[1] EFREI Paris, Villejuif, France
layth.sliman@efrei.fr, Benoit.charroux@efrei.fr
[2] IBISC Laboratory, Evry University, Evry, France
nazim.agoulmine@ibisc.univ-evry.fr

Abstract

Despite the spread of sharing economy platforms, as the best of our knowledge, no online solution has been proposed to handle the negotiation of new agreements and contracts between the participants in such platforms, which entails losing major business opportunities due to a lack of negotiation frameworks enabling mutual business and legal agreements. This paper describes an innovative smart contract-based negotiation framework integrated into sharing economy platforms to enable dynamic negotiation and electronic signature of digital agreements between partners. The proposed framework itself is technology agnostic. It can be used with any distributed collaborative platform regardless of the used technologies (web service, blockchain, etc.). We have used smart contract system as a mean to initiate and submit negotiated calls for tenders to respond to a business opportunity by multiple actors. The implementation uses the Orcha language, a new high-level smart contract language, to validate the framework concepts.

1 Introduction

New economic models are emerging in the global markets, such as demand-driven economy, virtual marketplaces, Crowd Funding, Crowd Sourcing, etc. These models are boost-up by the spread of ICT technologies [8]. These economic and technological forces are producing more and more complex systems, where the interconnection between actors, the availability of trusted information, as well as cost and revenue sharing among the actors are the key factors to obtain sustainable and cost-effective businesses. These systems require a decentralized yet trusted negotiation framework so that mutual agreements that govern the collaboration and the usage of the shared resources can be constituted, enforced, and verified. This is the case, for example, of the food delivery services, which are increasingly offered by the producers and vendors by externalizing the delivery dynamically using service registries such as Uber Eats, JustEat, TooGoodToGo... etc. The principles and techniques that appears to suit these applications better are the "decentralized consensus" (e.g. Blockchain) that allow participants on a distributed network to reach a perfect agreement on a shared resource. Even in the case of very simple multiple-actors infrastructures, as in some food chains, the value created in the short and medium time-horizon is sufficient to justify the introduction of the new technology while reducing the need for trust among the different partners [7] .

In this context, smart contracts is emerging as the disruptive technology able to fuel such systems characterized by multiple actors strongly interconnected while maintaining a low level of mutual trust. Smart contracts are decentralized and autonomous computer programs that are executed on the distributed ledger upon predefined events. However, despite its rapid development, this technology is still in its early stages of potential, it still presents some inherent defects which hiders its deployment in a factual project [4]. In particular, the possibility of integrating the business models, the choices, and the preferences of the different actors in the smart contract appears as a critical factor in democratizing more largely this technology.

The literature mainly considers the Business Process Modelling and Design for Blockchain-based solutions, which are then transformed into executable Smart Contracts [1] and [2]. Yet, the literature regarding the mutual definition by multiple actors of new smart contracts adapted to a particular need or business opportunities are quite limited [5]. In particular, to the best of our knowledge, no solutions have been proposed to handle the negotiation of new smart contracts to respond to business opportunities. To overcome this technical limitation, we describe an innovative smart contract-based negotiation mechanism that can be integrated into a blockchain. In particular, the presented solution introduces a smart contract system that is able to automatically launch and negotiate a call for tenders until completion (lifecycle management) to respond to a business opportunity by multiple actors.

This paper is organized as follows: in section 2, we present the concept of smart-contract as launched that is a cornerstone of the solution. Section 3 describes the proposed framework, which uses the smart contract language called Orcha[1]. After that, we present the implemented proof of concept system in section 4. Finally, we conclude and propose some perspectives to our work.

2 Smart Contracts

Smart contracts are programs coded with a programming language and executed in a runtime environment on a decentralized consensus system i.e. blockchain.

In the following, we briefly illustrate the smart contract programming and runtime environment focusing on Ethereum [3], a blockchain platform that was the first to introduce the smart contract concept.

Ethereum is a platform that intends to make a programming universe for the development, deployment, and execution of smart contracts for decentralized organizations over the blockchain. Ethereum integrates a Turing-complete programming language, called Solidity [3]. Solidity contains a set of instructions that enable arbitrary management of transactional states [6]. Solidity smart contracts are compiled into bytecode and encapsulated in Ethereum Virtual Machine (EVM). This later is intended to serve as a runtime environment for Solidity-based smart contracts. It focuses on providing a decentralized implement self-enforced smart contracts execution environment.

Finally, it is worth mentioning that each Ethereum node in the blockchain runs and maintains its own EVM implementation. EVM has been implemented in Python, Ruby, C ++, and some other programming languages [6].

Another language was specified by the Ethereum organization to respond to the Python language called Serpent. It is an Ethereum smart contract language that is close to Python. It is designed to encompass the benefits of Python in its simplicity, minimalism, and dynamic typing. When building the executable smart contract, serpent code is first compiled into LLL and then into bytecode for the EVM. The LLL name is diminutive to Low-Level Lisp-like Language. LLL refers to a language similar to Assembly that came to add a low-level layer into the EVM. The language adopts the syntax of Lisp. It is used when there is a need to deal

[1] https://github.com/orchaland/orchalang/tree/master/orchalang-spring-boot-autoconfigure/src/main/java/orcha/lang

with particular problems that are, by nature, low-level, e.g., require direct access to memory or storage.

The business logic that governs collaboration in a blockchain is supposed to be handled using smart contracts. However, the languages used to write smart contracts lack the elements necessary to negotiate dynamic business collaborations. This is due to the absence of interactions between the contractors (human and software) essential to defining collaborative business processes' functional and non-functional properties. Furthermore, current smart contract languages are very technical and do not incorporate business semantics, leading to a non-uniform interpretation of the smart contract by the different stakeholders. Consequently, it is crucial to define a new collaboration language tailored to the definition of smart contracts. Such a language should handle the complexity of the interactions between the different parties involved in a collaboration.

3 Framework Description

In the following, we introduce a new framework that helps construct and agree on a smart contract (called here contractualization process). We use also a novel high-level collaboration oriented smart contract language called Orcha [2] to validate the framework.

3.1 Orcha Language

Orcha is a business process modelling, deployment and coordination language developed by our team. It includes simple instructions that describes in a generic way business process activities. Orcha programs include a reduced number of instructions (Compute, Receive/From, Send/To, Condition, and When) represented by abstract syntax trees so that analysers can efficiently process them. Orcha contains a small and simple set of instructions designed to describe the answer of the essential questions around a collaborative process:

Who is involved? How an actor receives the needs to do the assigned tasks? When (time-wise and in which order) to do the task? What to do? With whom? On what? What external events should be taken into account? To whom, when and how produced events are sent?

The Orcha programs are event-based. They are triggered and run by events to manage the interactions between business processes human and virtual activities. They can be customized to any business field, i.e., the user according to their own business terminology can define the semantic of the instructions.

Rather than handling the specifications of individual tasks, Orcha allows to specify the data exchanged between during the coordination of activities. In that way, Orcha programs remain independent from any underlying technical implementations of tasks. In other words, in Orcha, there is a clear separation between the collaborative process (described in Orcha language) and the individual business tasks (that can be implemented in any other language). That is, Compute instruction in Orcha programs calls business services that implement individual business tasks.

An Orcha program describes eventually a business process, i.e., human actors, applications,

[2] https://github.com/orchaland/orchalang/tree/master/orchalang-spring-boot-autoconfigure/src/main /java/orcha/lang

and devices exchanging messages and coordinates their activities (Figure 1).

Orcha uses business terms to express the business process. For instance, a process to handle a passenger language delivery procedure in an airport could be:

```
receive passport from passenger
controlIdentity with passport.photo
receive luggage from agent
scanLuggage with luggage.value
when "scanLuggage fails and controlIdentity terminates"
alertAuthorities with controlIdentity.result
```

Business processes written in Orcha are executable programs. Consequently, one needs only to configure its Orcha program and simply run it to drive its business. The configuration defines the input and output data sources for Receive and Send instructions; for instance, (*receive order from customerBase*) and (*send order to customer by eMail*) as well as the service to be activated by the Compute instruction is running (compute service with...). Orcha programs perfectly match Smart Contract requirements in that they are event driven, decentralized and, portable (executed in their own containers). Orcha enables services applications and IoT devices integration. For instance, when you write: *receive passport from passenger*, data for the passenger can come from Sensors, SQL and NoSQL databases or files. Similarly, the control service in *controlIdentity with passport.photo* can be a remote Service or a local application. A Smart Contract written in Orcha is compiled using the following steps: preprocessing, lexical analysis, syntax analysis, grammatical analysis, post-processing, linkage, and output generation (generate a Spring Integration Java program).

3.2 Contractualization of smart-contracts

In this section, we describe a contractualization framework that enables collaborators to dynamically create a smart contract to quickly respond to a business opportunity. In this framework, collaborators submit and respond to tenders via an IHM that allows to specify the needs. As a result, a smart contract representing the collaboration process is dynamically created. The framework is described in Figure 1. As highlighted, in the framework:

- A customer defines its needs and specifies the desired outcomes.
- The customer sends a Call for Tender (CfT) to the contract ledger workplace.
- Providers can retrieve the CfT and formulate a response as a Tender Proposal (TP),
- TP is sent to the customer.
- Customer retrieves the TP and either;
- It validates and diffuses it in the blockchain or;
- It can re-formulate a new CfT based on the received TP. In this case;
- The process restarts again until an agreement is reached.

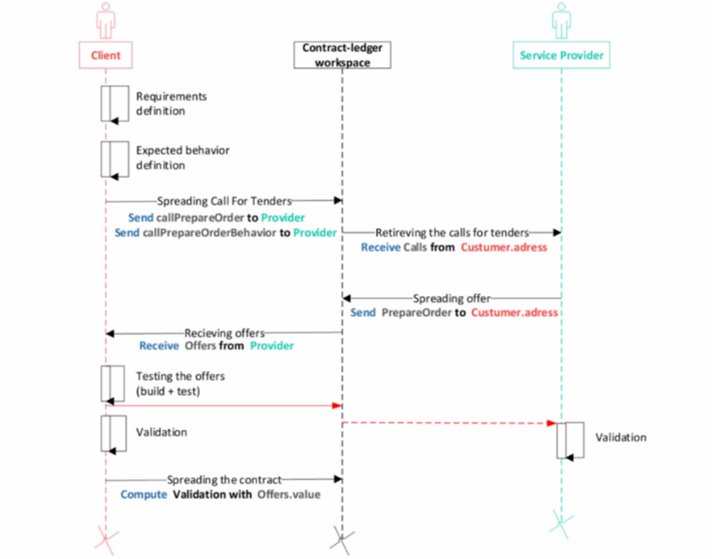

Client
Contract-ledger workspace
Service Provider
Requirements definition
Expected behavior definition
Spreading Call For Tenders
Send callPrepareOrder to Provider
Send callPrepareOrderBehavior to Provider
Retireving the calls for tenders
Receive Calls from Custumer.adress
Spreading offer
Send PrepareOrder to Custumer.adress
Recieving offers
Receive Offers from Provider
Testing the offers (build + test)
Validation
Validation
Spreading the contract
Compute Validation with Offers.value

Figure 1: Sequence Diagram Describing the Contractualization Process

The obtained smart contract is signed by all stakeholders involved in the collaboration to confirm and maintain an inviolable record of the collaborators' contractualization. It is then submitted to the blockchain to be validated via the consensus mechanism. As a result of the consensus, if the smart contract is approved, it is added to the blockchain as a definitive transaction.

In the end, according to the conditions agreed by the collaborators, the smart contract is executed. Its execution creates new transactions that must be added to the blockchain by a consensus mechanism.

It is worth mentioning that the contractualization process itself is represented as a smart contract that uses Orcha as a language to specify the exchanging calls and responses of tenders. To this end, an interactive Shell interface for users to launch a call for tenders or respond to tenders is defined.

3.3 Proof of Concept Implementation

In this section we will present a proof of concept (PoC) that demonstrates this framework's feasibility. The PoC is implemented on the Git version control system. Git was selected because of its similarity to blockchain in terms of versioning mechanism based on hash functions, its distributed storage, and its pseudo decentralization.

The PoC considers a simple collaboration case where a client and a set of sub-contractors can interact to contract a service (as highlighted in Figure 2).

In the following, we explain the business logic implemented by presenting Orcha commands customized to cover the exchanges necessary for contractualization and the technical architecture that allowed us to make the command shell.

To start a collaboration simulation, a client who needs a service must create a git directory with public access as a distributed Smart-Contract registry. He/she then enters the address of this directory in the contracting system. From this moment, the client can issue a call for tenders. A call for tenders is a file that includes the customer's needs as well as the expected

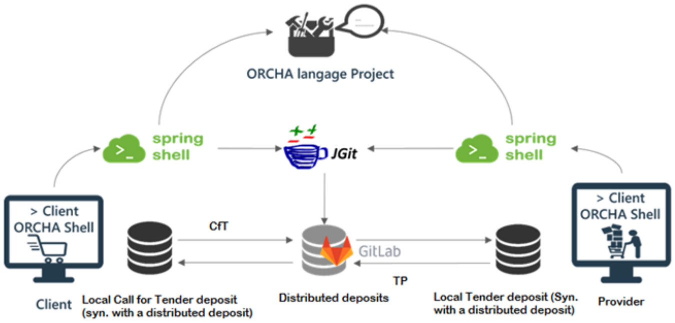


Figure 2: Technical architecture of the proof of concept

behavior of the service providers' responses. The file, written in Orcha, is completed with additional configuration files and a set of input/output data representing the desired service outcome.

Service providers must respond to a request for a proposal that interests them, create a branch on the collaboration's directory, and deposit the Orcha program of their offer. Similarly, as for the call for tenders, the program is accompanied by the configuration and data files.

After analyzing and testing the various response received, the client selects one or more offers. The customer will have, at this time, all the necessary information to write a complete smart-contract that would correctly govern future collaborations.

If an offer does not fully match the client's preferences, the client may continue a back-and-forth exchanging with the supplier to negotiate the terms.

A) Shell orders made for the contractualization phase

The distributed registry of each user's smart-contract contains the folder named "Business" that includes the following main folders:

- "myCallsForTenders": intended to include the calls for tenders sent by the customer;
- "myOffers": intended to include the offers provided by the service provider;
- "receivedCallsForTenders": If the user is a service provider, he or she will receive customer calls for tenders on this folder.
- "receivedOffers": If the user is a customer who has issued the CfT, he will receive the service provider response files on this folder.

In the following, we explain the different commands that we defined using Orcha language to enable a customer to interact with providers during the contractualization process:

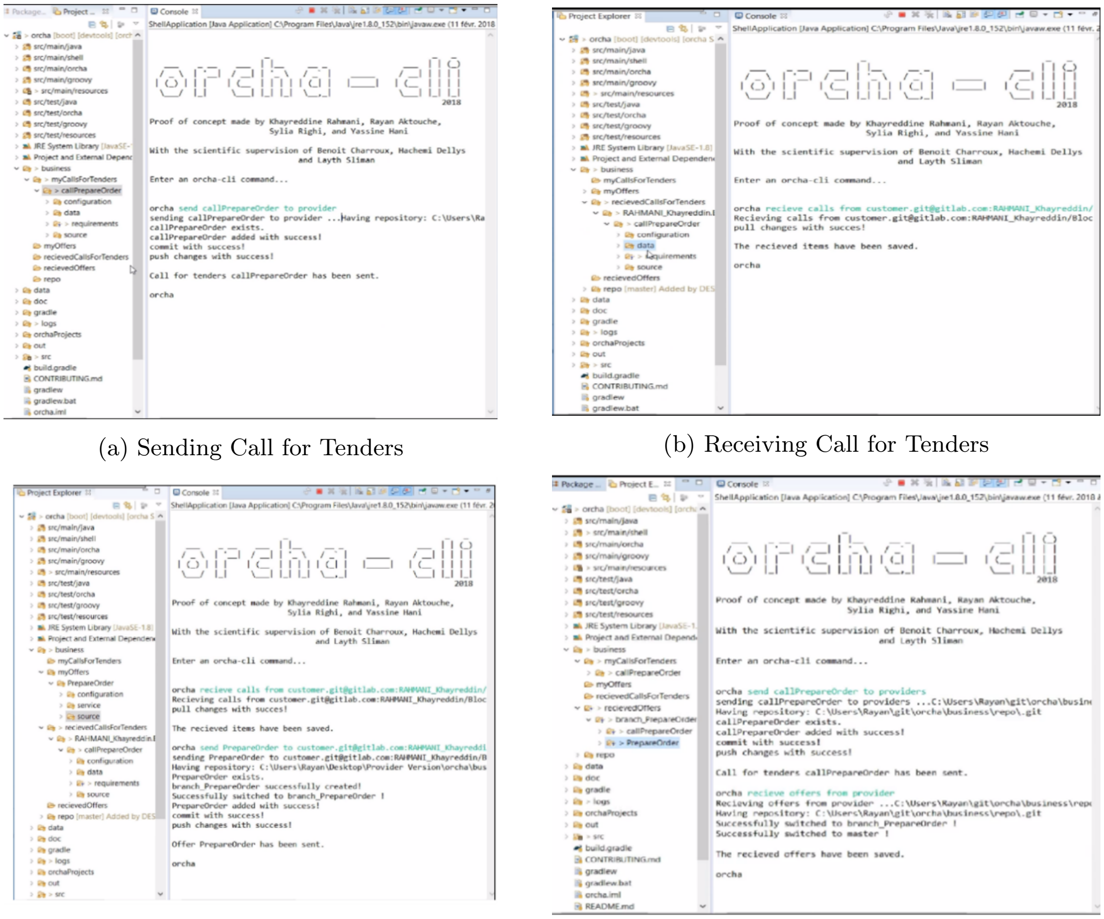
i. **Command 01 : Distribution of a call for tenders - customer order**

Orcha > send callForTender to providers.

This command allows a client to broadcast the "call for Tender" call for tender written in ORCHA language, which it has deposited in the "my Calls For Tenders" folder.

ii. **Command 02: Reception of a Request for Proposal - Service Provider Order**

Orcha > recieve calls from customer.customer@



```
ShellApplication [Java Application] C:\Program Files\Java\jre1.8.0_152\bin\javaw.exe (11 févr. 2018

                                                                    2018
Proof of concept made by Khayreddine Rahmani, Rayan Aktouche,
                         Sylia Righi, and Yassine Hani

With the scientific supervision of Benoit Charroux, Hachemi Dellys
                               and Layth Sliman

Enter an orcha-cli command...


orcha send callPrepareOrder to provider
sending callPrepareOrder to provider ...Having repository: C:\Users\Ra
callPrepareOrder exists.
callPrepareOrder added with success!
commit with success!
push changes with success!

Call for tenders callPrepareOrder has been sent.

orcha
```

(a) Sending Call for Tenders

```
ShellApplication [Java Application] C:\Program Files\Java\jre1.8.0_152\bin\javaw.exe (11 févr. 2

                                                                    2018
Proof of concept made by Khayreddine Rahmani, Rayan Aktouche,
                         Sylia Righi, and Yassine Hani

With the scientific supervision of Benoit Charroux, Hachemi Dellys
                               and Layth Sliman

Enter an orcha-cli command...


orcha recieve calls from customer.git@gitlab.com:RAHMANI_Khayreddin/
Recieving calls from customer.git@gitlab.com:RAHMANI_Khayreddin/Bloc
pull changes with succes!

The recieved items have been saved.

orcha
```

(b) Receiving Call for Tenders

```
ShellApplication [Java Application] C:\Program Files\Java\jre1.8.0_152\bin\javaw.exe (11 févr. 2

                                                                    2018
Proof of concept made by Khayreddine Rahmani, Rayan Aktouche,
                         Sylia Righi, and Yassine Hani

With the scientific supervision of Benoit Charroux, Hachemi Dellys
                               and Layth Sliman

Enter an orcha-cli command...


orcha recieve calls from customer.git@gitlab.com:RAHMANI_Khayreddin/
Recieving calls from customer.git@gitlab.com:RAHMANI_Khayreddin/Bloc
pull changes with succes!

The recieved items have been saved.

orcha send PrepareOrder to customer.git@gitlab.com:RAHMANI_Khayreddi
sending PrepareOrder to customer.git@gitlab.com:RAHMANI_Khayreddin/B
Having repository: C:\Users\Rayan\Desktop\Provider Version\orcha\bus
PrepareOrder exists.
branch_PrepareOrder successfully created!
Successfully switched to branch_PrepareOrder !
PrepareOrder added with success!
commit with success!
push changes with success!

Offer PrepareOrder has been sent.

orcha
```

(c) Call for Tenders response

```
ShellApplication [Java Application] C:\Program Files\Java\jre1.8.0_152\bin\javaw.exe (11 févr. 2018 à

                                                                    2018
Proof of concept made by Khayreddine Rahmani, Rayan Aktouche,
                         Sylia Righi, and Yassine Hani

With the scientific supervision of Benoit Charroux, Hachemi Dellys
                               and Layth Sliman

Enter an orcha-cli command...


orcha send callPrepareOrder to providers
sending callPrepareOrder to providers ...C:\Users\Rayan\git\orcha\busine
Having repository: C:\Users\Rayan\git\orcha\business\repo\.git
callPrepareOrder exists.
callPrepareOrder added with success!
commit with success!
push changes with success!

Call for tenders callPrepareOrder has been sent.

orcha recieve offers from provider
Recieving offers from provider ...C:\Users\Rayan\git\orcha\business\repo
Having repository: C:\Users\Rayan\git\orcha\business\repo\.git
Successfully switched to branch_PrepareOrder !
Successfully switched to master !

The recieved offers have been saved.

orcha
```

(d) Call for Tenders Proposal acceptance

Figure 3: Contractualization framework implementation

This command allows a service provider to receive calls from the customer with the address "customer @" on his local copy of the distributed registry.

iii. **Command 03: Sending an offer - order service provider**

Orcha > send offerSP1 to customer.customer@

This order allows a service provider to offer their "offerSP1" offer to the customer with the address "customer @"

iv. **Command 04: tenders receiption - sales order**

Orcha > recieve offers from providers

This order allows a customer to receive the various "offer" offers offered by service providers "providers"

v. **Command 05 : Validation of an offer - customer order**

Orcha > send validation to providers.branchName

This command allows a customer to validate an offer he has received from a service provider on the branchName branch

B) **Technical architecture of proof of concept of contractualization**

The proof of concept is structured in the form of a client application based on shell commands orchestrating the different exchanges that perform the contractualization (Figure 2). The implementation of shell commands is done using SpringShell. Behind these commands, the sending and receiving operations are done by the encapsulation of Git functions, called from the Java environment using the JGit library, which acts on Gitlab hosted repositories [3] (see Figures 3).

4 Conclusions

In this paper, we introduced a new framework for smart contract negotiation. The framework follows Call for Tenders' business logic. It enables customers and providers to settle smart contracts in a negotiated way so that they can quickly respond to business opportunities. The framework has been validated using Orcha Language, a new high-level smart contract language. A Proof of Concept (PoC) has been implemented to assess the feasibility of the framework. The PoC used Git as the underlying platform. This latter has been chosen due to its similarity to blockchain logic. The PoC has shown that the concepts introduced by the framework are sound and permits it objectives. In future works, we aim to implement the framework using a real blockchain and a full smart contract lifecycle.

References

[1] Miguel Pincheira Caro, M. S. Ali, M. Vecchio, and R. Giaffreda. Blockchain-based traceability in agri-food supply chain management: A practical implementation. *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany)*, pages 1–4, 2018.

[2] Roberto Casado-Vara, Alfonso González Briones, Javier Prieto, and Juan Corchado Rodríguez. *Smart Contract for Monitoring and Control of Logistics Activities: Pharmaceutical Utilities Case Study*, pages 509–517. 06 2019.

[3] Kevin Delmolino, Mitchell Arnett, Ahmed Kosba, Andrew Miller, and Elaine Shi. A programmer's guide to ethereum and serpent. *URL: https://mc2-umd. github. io/ethereumlab/docs/serpent_ tutorial. pdf.(2015).(Accessed May 06, 2016)*, pages 22–23, 2015.

[4] Deloitte. global blockchain survey. breaking blockchain open. 2018.

[5] Valentina Gatteschi, F. Lamberti, Claudio Demartini, Chiara Pranteda, and Victor Santamaria. To blockchain or not to blockchain: That is the question. *IT Professional*, 20:62–74, 03 2018.

[6] Yoichi Hirai. Defining the ethereum virtual machine for interactive theorem provers. In *International Conference on Financial Cryptography and Data Security*, pages 520–535. Springer, 2017.

[7] Guido Perboli, Stefano Musso, and Mariangela Rosano. Blockchain in logistics and supply chain: A lean approach for designing real-world use cases. *IEEE Access*, 6:62018–62028, 2018.

[8] Roberto Tadei, Edoardo Fadda, Luca Gobbato, Guido Perboli, and Mariangela Rosano. An ict-based reference model for e-grocery in smart cities. In *International Conference on Smart Cities*, pages 22–31. Springer, 2016.

[3] visit https://www.youtube.com/watch?v=RSKe9oxuJfM

An Architecture Proposal for E-health Data Collection and Storage Based on Internet of Things and Blockchain

Alan Nascimento Gomes[1] and Emanuel Ferreira Coutinho[1]

Federal University of Ceara (UFC), Quixadá, Ceará, Brazil
alanng@alu.ufc.br,emanuel.coutinho@ufc.br

Abstract

Currently, several technologies are being used together to improve the quality of services for people. Specifically for the health area, the application possibilities involving both software and hardware are quite diverse. Internet of Things (IoT) and blockchain are two technologies that are currently integrating more and more to provide better services, taking advantage of their characteristics. This work proposes an architecture for the collection and storage of e-health data, based on IoT and blockchain. For its validation, a prototype was designed and the flow of operations was analyzed. Preliminary results indicated the proposed architecture has the potential to integrate IoT and blockchain to support e-health applications, enabling research and application development, but a broader study with IoT devices is needed for a better assessment.

1 Introduction

With the integration of technologies such as Internet of Things (IoT) and blockchain, a new computational layer has emerged capable of offering secure data sharing and analysis, in addition to enabling privacy guarantees, where it is possible to authenticate, authorize, control and audit the data obtained from sensors [1]. In this context, the integration of these technologies has enabled the development of applications in different sectors: finance, health, education, etc.

IoT is a paradigm in which heterogeneous physical objects are interconnected through wired or wireless technologies. The basic idea is to integrate "things" on the Internet by providing users with various services [2][3]. Nowadays, many IoT projects have milions of IoT devices acting as sensor or actuator, collecting sensitive data from people or processing this data for the most varied purposes [4].

According to the *Healthcare Information and Management Systems Society* (HIMSS) [5], e-health is defined as the application of the Internet and other related technologies in the health sector to improve access, efficiency and the effectiveness of the quality of clinical processes and business processes used by healthcare organizations, professionals, patients and consumers, in an effort to improve the health status of patients.

In the literature, several works have invested in e-health applications [6][7]. Neto et al. [7] proposed an approach for monitoring people who are part of risk groups. For example, sedentary people, using IoT technologies. They monitored users' physiological data through wearable devices and sends this data to a computational cloud. These data are processed, stored and presented to the healthcare professional, who will monitor and establish new activities for the user. They built a mobile and web applications, and collected data from sensors and a dataset of health data. Neto et al. [6] presented an IoT approach to help sedentary people. This approach monitors users' physiological data through wearable devices and sends them to the cloud for processing. In the cloud, the data is processed and presented to the health professional, that will monitor and establish new activities for users. The data generated in situations such as those described in these works brings the problem of how to access the data safely and how to avoid falsification.

Blockchain is a data structure that makes it possible to create a transaction-proof digital ledger and share it [8]. This technology uses public key cryptography to sign transactions between the parties. The transactions are then stored in a distributed ledger. The ledger consists of cryptographically linked transaction blocks, which form a blockchain [9].

The data obtained from the sensors when stored in centralized bases can cause several problems due to this centralized topology. Among the problems, we highlight those related to security, for example, when there is a server failure or when the server suffers hacker attacks. Blockchain shows itself as a potential technology to solve these problems by offering desired resources for large-scale IoT infrastructures, such as decentralization, reliability, traceability and immutability [10].

The objective of this work is to present an architecture that integrates IoT and blockchain technologies. A flow of operations from the collection of sensors data to the availability of this data in a web / mobile application will be described. An application prototype to validate the architecture will also be presented in the work.

This work is divided into the following sections: Section 2 shows some related work; in Section 3 the proposed architecture is presented; Section 4 shows the design of a proof of concept for the architecture, the developed prototype and some discussion; and finally, Section 5 presents the conclusions and future work.

2 Related Work

Some works in the literature have developed research related to IoT and blockchain [10][11][12]. Wang et al. [10] proposed a hierarchical blockchain storage structure, where the majority of blockchain is stored in the cloud, while the most recent blocks are stored in an overlay network. Research opportunities with the use of blockchain technology in applications that manipulate DNA sequence data were presented in Neto et al. [12]. For this, an architecture for general e-health applications with blockchain was proposed. They also implemented a proof of concept to analyze the use of blockchain technology in e-health applications using DNA sequence data and they also listed a set of research opportunities. A study of the use of blockchain technology in an e-health approach was described in Neto et al. [11], using the distributed database BigchainDB, where a performance analysis of transaction validation times was conducted.

Chendeb et al. [13] proposed a multi-layer IoT/blockchain based architecture customized and designed to be used in the medical field. Many parties interact With this information, including doctors, health service providers, insurance companies and pharmacies. A distributed blockchain cloud architecture model was designed to meet the design principles required to efficiently manage the raw data streams produced by numerous IoT devices, promoting the possibility of using blockchain technology with IoT and vertical applications. The proposed architecture was designed to support high availability, real-time data delivery, high scalability, security, resiliency, and low latency. As future work, the authors intent to implement this architecture in a real system, and evaluate performance.

Batista et al. [4] proposed Heimdall, a distributed smart contract-based framework that provides access control for sensitive or personal data collected by IoT devices that follow the prerogatives of General Data Protection Regulation (GDPR) and General Data Protection Law (Lei Geral de Proteção de Dados - LGPD). The users must be able to: authorize or revoke the data access without depends on a trusted third party; to define what subset of your sensitive or personal data may be accessed or not based on access rules; to audit whom accessed his sensitive or personal data and be able to see when this occurred. For this, it is necessary develop a smart contract that rules the access control, create the protocol that defines the possible operations on the access control framework and the involved actions, define the syntax and semantics of access rules, design a distributed mechanism to verify the access rules and create a multidimensional index of sensitive and personal data to facilitate queries on stored data. This work is still in development.

3 Architecture Proposal

This section describes the main elements of the proposed architecture. These elements can be composed of sub-elements of hardware or software systems.

Figure 1 represents the proposed architecture and operations flow of an environment that uses IoT and blockchain technologies. The proposed scenario illustrated by the architecture is an e-health application, with the purpose of verifying the health status of a patient.

At a high level, the first element is the set of devices responsible for performing measurements and data capture. For an e-health environment, for example, these devices are sensors responsible for analyzing the patient's physiological events, such as temperature sensors, blood pressure, glucose, etc. The second element is the communication system used to transmit data from the input devices to a storage environment. The third element is the data management system, which is related to the machines responsible for processing, storing and retrieving the data. And finally, the applications responsible for making interactions of the system with users capable of verifying the health status compose the fourth element.

In item (1) it is possible to view an IoT prototype responsible for collecting the data, in addition to elements responsible for handling the data coming from the sensors and preparing them for sending to the server intended to carry out the storage on the blockchain. Item (2) presents the architecture element responsible for communicating the IoT Prototype with the server's itens. In item (3), server P will receive the data read from the patient's health status and perform the insertion of the data on the blockchain. In item (4), the server C responsible for reading the blockchain data is shown. Sub-items (5.1) and (5.2) show the applications that access blockchain data through the server C, which make up the set of applications in item (5). And sub-items (6.1) and (6.2) are the individuals who have access to the applications.

4 Proof of Concept, Application and Discussion

This section presents a proof of concept of the proposed architecture and an application to illustrate a possible e-health application scenario. At the end, some discussions about architecture and technology are presented.

4.1 Proof of Concept

In this section, the implementation of the architecture presented in the previous section will be discussed. For this, an IoT prototype was designed and built in a similar way to that presented in item 1 of Section 3, where the sensors used for the implementation were simulated in order to generate data regarding the measurement of body temperature, blood oxygen level and heart rate.

The used development board was Esp8266 Nodemcu wifi module, responsible for receiving health status data and connecting to the Fiware framework. This framework is used to allow the

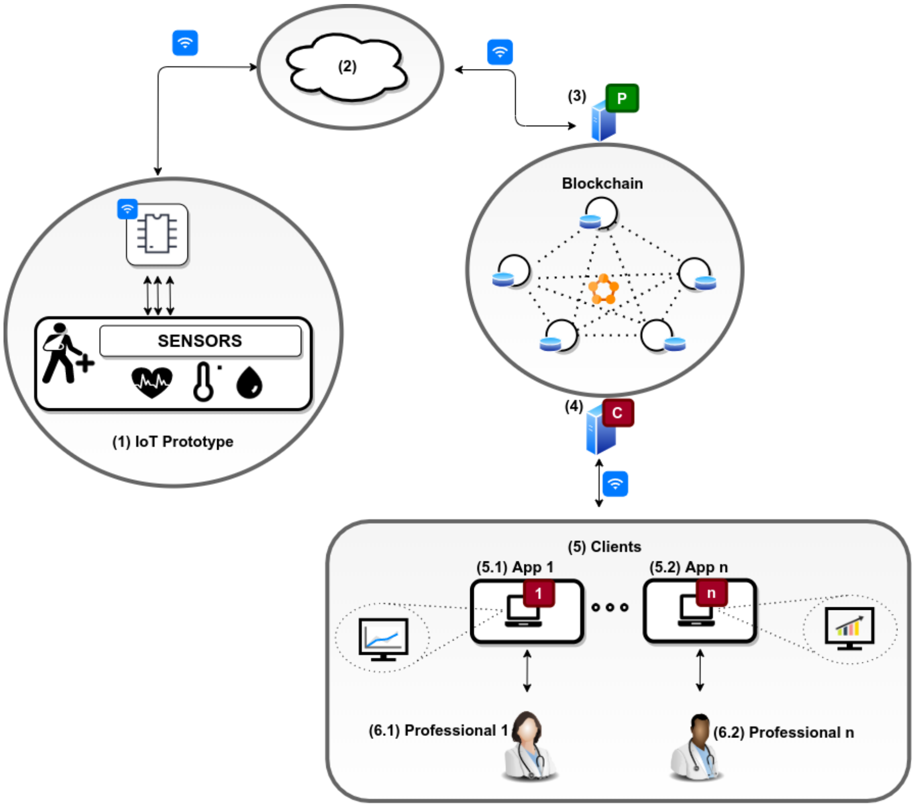


Figure 1: Architecture proposal

system to become scalable and to be able to deal with heterogeneity when the system becomes more robust [14]. Fiware is an open source project that provides a set of components whose objective is to facilitate the development of intelligent applications. It emerged in Europe from the Future Internet Public Private Partnership (FI-PPP), defining APIs for the development of solutions in several sectors, such as: smart cities, agriculture, e-health, transport and energy [15][16]. A simplified view of the components to perform the communication is shown in Figure 2.

In Figure 2, the implementation of items 1, 2 and 3 of Figure 1 is presented and the blocks will be described below. The main component of Fiware middlwware is presented in the block referring to Orion Context Broker, responsible for managing context information, such as: updates, queries, records and subscriptions [17]. The context information in the scenario presented refers to the patient's health status. For this architecture, Orion Broker will receive notifications from Agent IoT informing context updates.

The IoT Agent component presented in the block diagram has the function of communicating the physical devices with the Orion Broker, because in an IoT system it is common to have a diversity of technologies and communication protocols, requiring an entity responsible for carrying out the interpretation of data from the sensors for the Orion Context Broker. This component also addresses security issues and provides services for programmers AGENT. In this architecture, Agent IoT will listen to the MQTT Broker so that the measurements can be sent to Orion.

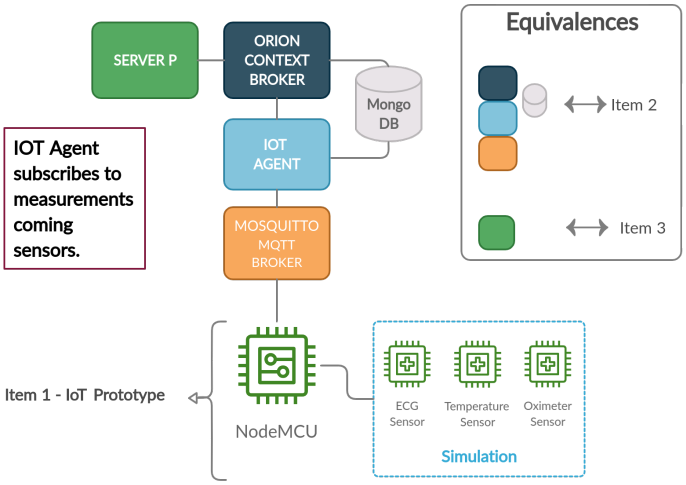


Figure 2: Simplified view of the components to perform the communication

In addition, Orion Context Broker uses the MongoDB database to store information related to the context state of devices across entities. These states are stored in the JSON format [18].

With Orion Broker, it is possible for asynchronous notifications to be sent to applications connected to the Broker. This is made possible when applications subscribe to receive update notices. This makes it possible for applications that communicate with the Orion Context Broker do not make requests unnecessarily, but only when the context of an entity is updated. The use of the signature mechanism will therefore reduce the volume of requests and the amount of data transmitted between the components of the system. This reduction in network traffic will improve overall responsiveness [19]. Therefore, whenever a change in the patient's health status occurs, a POST request is submitted to the server P, in order to update the patient's information.

Regarding the section of architecture dedicated to data storage, the types of available blockchains were initially analyzed. Blockchain networks are divided into two groups based on the type of permission, which are: without permission (permissionless) and with permission (permissioned). An example of a blockchain network without permission is Bitcoin, in which topology block insertion in the network is not restricted. However, this approach does not satisfy the requirements of the implemented scenario, as the data related to health are of a private nature. In blockchains with permission only individuals with authorization can interact with the network [20]. This type of network is interesting for the implemented scenario because the access to patient data is limited.

The solution for using a permissioned blockchain was to use Hyperledger [21]. The Linux Foundation launched this project in 2015, which built a corporate blockchain development platform [22]. Hyperledger Fabric is a technology from Hyperledger technologies. It uses a modular structure to provide scalable components, including encryption, authentication, consensus algorithm, smart contract, data storage and other services [23]. Chaincodes are the smart contracts responsible for allowing applications to interact with the network, depending on the business rule of the application. For this architecture, in the chaincodes functions were defined that insert the data in the blockchain, the reading of the network data, through the servers P and

C respectively, and the search of the data history.

With the data inserted in the Hyperledger network, it is already possible for applications to make requests in order to obtain the data from the sensors and present them in a more readable way. For the demonstration of this architecture, the servers P and C were implemented in Node JS and the application responsible for demonstrating the data in Vue JS.

4.2 Application

In this section, the prototype of the WEB application will be described. We highlight here that the idea is to have an application that is an e-health application scenario just to illustrate the architecture.

This application initially aims to display graphs of the patient's situation, based on three variables indicating: heart rate, body temperature and blood oxygen level. The values of these variables are obtained from the Hyperledger network and are changed by the simulated sensors, as previously discussed. In the proposed scenario, only one patient is being considered, whose identification is being named by the identification 111.111.111-11.

As the used network ledger is immutable and transparent, it is possible to take advantage of these characteristics to track transactions and thus obtain the current status and history of the patient's vital signs. Figure 3 shows the last data stored in the network regarding measurements that indicate heart rate (92 beats per minute), temperature (37 degrees) and blood oxygen saturation (98%). This chart can be used by professionals to facilitate visualization of the patient's current situation through the measured values. This would be just a possible feature of the application. E-health applications have many features and depend a lot on the type of application or area of expertise. As patient data is stored on the blockchain, its origin is transparent to the end user.

Figure 4 displays the data history. These data are: timestamp, name, docType, ekg, temperature and oxymeter. These data represent the timestamp in which the transaction was performed by the network nodes, the patient's name, an identifier of the type of transaction, the measured heart rate value, body temperature and blood oxygen rate, respectively. This is a code vision. The final user did not visualize this information in this format. This history is obtained by the server C from Figure 1, which makes a request to the Hyperledger network to obtain an array that is formed by the values of the vital data and time stamps, this array is built based on the patient's identifier. Data of ekg, temperature and oxymeter are displayed in the graphs of Figure 3.

Finally, in Figure 5, the line graphs show samples of the data history. These graphs were constructed with the values similar to those in Figure 4. Through them it is possible to investigate individually and together the three variables that are being measured by the sensors. Thus, it is easier for the application user to study the patient's situation, through the knowledge of the behavior of these data in the past, since it is possible to easily examine the trajectory of the variation of the information obtained from the sensors according to the evolution of the time that is in the horizontal axis. And by selecting one of the markers, users are provided with an immediate visualization of the absolute values measured at each instant, as shown in Figure 5.

The line graph consists of the presentation of three variables: the upper line (orange and dotted) shows the measured values referring to the percentage of oxygen in the blood, the intermediate line (blue and continuous) refers to the value obtained from the ECG sensor, and the bottom line (green and dotted) is body temperature. The variation of the horizontal axis indicates the displacement in time and variations in the vertical axis define the measured value

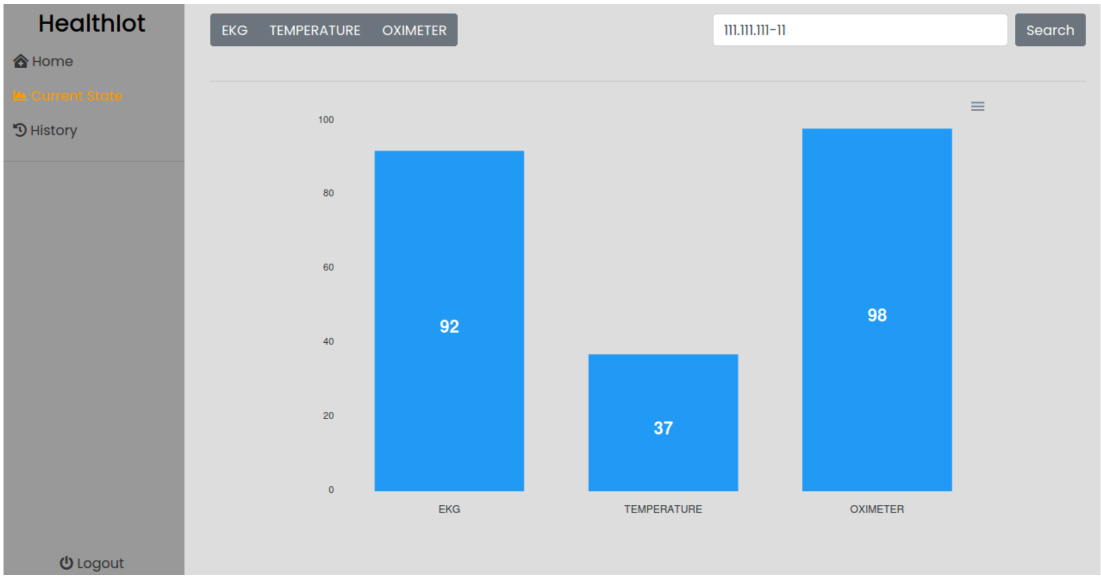
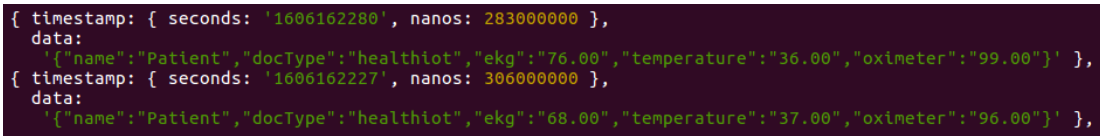


Figure 3: Measuring sample



```
{ timestamp: { seconds: '1606162280', nanos: 283000000 },
  data:
   '{"name":"Patient","docType":"healthiot","ekg":"76.00","temperature":"36.00","oximeter":"99.00"}' },
{ timestamp: { seconds: '1606162227', nanos: 306000000 },
  data:
   '{"name":"Patient","docType":"healthiot","ekg":"68.00","temperature":"37.00","oximeter":"96.00"}' },
```

Figure 4: Hyperledger network data

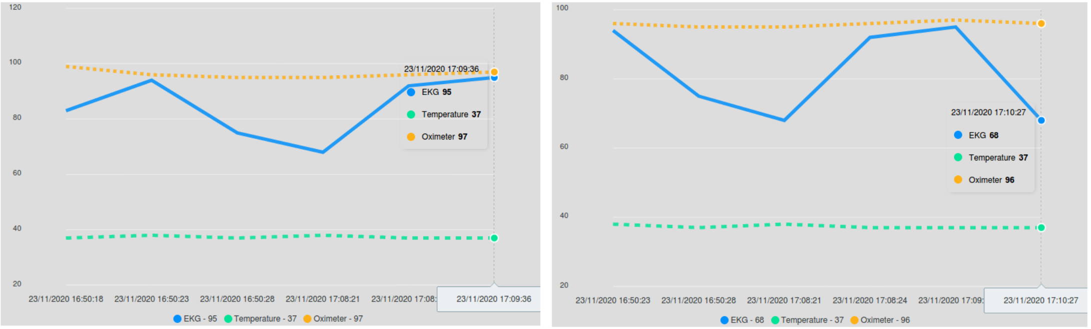


Figure 5: Samples of history captured from the sensors

for each variable.

The application presented in this section aims to validate the architecture discussed previously, indicating that with the implementation of the system through technologies for data collection, communication, storage, processing and presentation, it is possible to confirm that the components and the flow of operations established in the Figure 1 can be implemented and executed together.

4.3 Analysis and Discussions

As previously informed, there was no implementation of the architecture with all the items. In this case, the capture of sensor values was simulated, consisting of a work limitation. However, this does not invalidate the work as the flow of operations remains.

The application considered the use of a permissioned blockchain, that is, for e-health applications it would be better if the blockchain infrastructure was controlled with permissions for the involved institutions. In this case, Hyperledger was used for that purpose.

Several data are generated by the sensors, and the volume is often large. However, not all data makes sense to be stored on the blockchain. This is a research challenge, which involves data selection and merging, as the blockchain's storage capacity is limited. To get around this situation, relational databases can be used as a complement to the applications.

Regarding the financial cost, storing the data on a public blockchain would have an associated cost. This was yet another reason to use a permissioned and private blockchain. However, there is a cost to maintain the infrastructure between the involved institutions.

In order to fully serve a real e-health application, further study on the e-health sub-areas to be used is still needed. There are many sub-areas, so the number of features is also high. The integration between different systems and between different data formats also becomes a challenge, especially when considering issues of performance and quality of service. In this scenario, the use of IoT and blockchain must be carefully designed so as not to harm the entire e-health environment.

5 Conclusions and Future Work

This work presented an architecture for integrating IoT and blockchain. Thus, with its implementation, it will be possible to perform the flow of operations from the collection of data originating from sensors to its availability through a web or mobile application. A prototype of an e-health application was developed to validate parts of the architecture.

This work contributes to the spread of blockchain technology and its application. In addition, the proposed architecture can be applied to several domains using IoT and blockchain. This work is at an early stage, and it is possible to try several technologies related to IoT and blockchain. There is a need to have a deeper study on the integration of actuating and sensing devices to further characterize the relationship with IoT, and how data can be stored on the blockchain. It is also necessary to have a study more appropriate to e-health applications, so that prototypes can be developed that benefit well from the technologies involved. All of these tasks consist of future work.

Also as future work, we intend to fully implement the architecture in a more robust e-health application and consequent performance evaluation. For its evaluation, this will initially occur through the use by users specialized in e-health and also an analysis of application performance according to different workloads applied to the environment.

Acknowledgments: This work was supported by PIBIC 2020/2021 (01/2020) program, project **Integração de Aplicações E-health com Ambientes de Computação em Nuvem e Blockchain**, from Federal University of Ceará (UFC).

References

[1] Fabíola Greve, Leobino Sampaio, Jauberth Abijaude, Antonio Coutinho, Ítalo Valcy, and Sílvio Queiroz. *Blockchain e a Revolução do Consenso sob Demanda*, chapter 5, pages 1–52. Sociedade Brasileira de Computação (SBC), Maio 2018.

[2] Yongqing Zhu Quanqing Xu, Khin Mi Mi Aung and Khai Leong Yong. *A Blockchain-Based Storage System for Data Analytics in the Internet of Things*, pages 119–138. Springer International Publishing AG, 2018.

[3] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787 – 2805, 2010.

[4] Bruno L. A. Batista, Jose Neuman de Souza, and Joaquim Celestino Junior. Heimdall: An authorization framework based on blockchain for sensitive data access. *8th Internacional Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE)*, Jan 2020.

[5] HIMSS. Himss - healthcare information and management systems society — himss. https://www.himss.org/, 2019. 2020-01-22.

[6] Mauricio Moreira Neto, Emanuel Ferreira Coutinho, Matheus Roberto Oliveira, Leonardo O. Moreira, and Jose Neuman de Souza. Asp: An iot approach to help sedentary people. *6th Internacional Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE)*, Jan 2018.

[7] M. M. Neto, E. F. Coutinho, L. O. Moreira, J. N. de Souza, and N. Agoulmine. A proposal for monitoring people of health risk group using iot technologies. In *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–6, Sep. 2018.

[8] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[9] Nir Kshetri. Can blockchain strengthen the internet of things? pages 68–72, July/August 2017.

[10] G. Wang, Z. Shi, M. Nixon, and S. Han. Chainsplitter: Towards blockchain-based industrial iot architecture for supporting hierarchical storage. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 166–175, July 2019.

[11] Maurício Moreira Neto, Emanuel Ferreira Coutinho, Leonardo Oliveira Moreira, and José Neuman de Souza. Toward blockchain technology in iot applications: An analysis for e-health applications. In Augusto Casaca, Srinivas Katkoori, Sandip Ray, and Leon Strous, editors, *Internet of Things. A Confluence of Many Disciplines*, pages 36–50, Cham, 2020. Springer International Publishing.

[12] M. M. Neto, C. S. d. S.Marinho, E. F. Coutinho, L. O. Moreira, J. d. C. Machado, and J. N. d. Souza. Research opportunities for e-health applications with dna sequence data using blockchain technology. In *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*, pages 95–102, March 2020.

[13] Nada Chendeb, Nour Khaled, and Nazim Agoulmine. Integrating blockchain with iot for a secure healthcare digital system. *8th Internacional Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE)*, Jan 2020.

[14] FIWARE FOUNDATION. Fiware catalogue, 2018. https://www.fiware.org/developers/catalogue/.

[15] FIWARE FOUNDATION. Developers, 2019. https://www.fiware.org/developers.

[16] EUROPEAN COMMISSION. The future internet platform fiware, 2018. https://ec.europa.eu/digital-single-market/en/future-internet-public-private-partnership.

[17] FIWARE FOUNDATION. Welcome to orion context broker, 2018. https://fiware-orion.readthedocs.io/en/latest/index.html.

[18] FIWARE FOUNDATION. Iot over mqtt, 2018. https://fiware-tutorials.readthedocs.io/en/1.0.0/iot-over-mqtt/index.html.

[19] FIWARE FOUNDATION. Subsctiption, 2018. https://fiware-tutorials.readthedocs.io/en/1.0.0/subscriptions/index.html.

[20] K. Wüst and A. Gervais. Do you need a blockchain? In *2018 Crypto Valley Conference on*

Blockchain Technology (CVCBT), pages 45–54, 2018.

[21] The Linux Foundation. Hyperledger, 2020. https://www.hyperledger.org/.

[22] V. Aleksieva, H. Valchanov, and A. Huliyan. Implementation of smart-contract, based on hyperledger fabric blockchain. In *2020 21st International Symposium on Electrical Apparatus Technologies (SIELA)*, pages 1–4, June 2020.

[23] Hyperledger Fabric. Hyperledger fabric model, 2020. https://hyperledger-fabric.readthedocs.io/en/release-2.2/fabric_model.html.

BAMSim Simulator

Rafael F. Reale[2], Walter P. Neto[1], and Joberto S. B. Martins[1]

[1] Salvador University (UNIFACS), wcpneto@gmail.com, joberto.martins@unifacs.br
[2] Federal Institute of Bahia (IFBA), reale@ifba.edu.br

Abstract

Resource allocation is an essential design aspect for current systems and bandwidth allocation is an essential design aspect in multi-protocol label switched and OpenFlow/SDN network infrastructures. The bandwidth allocation models (BAMs) are an alternative to allocate and share bandwidth among network users. BAMs have an extensive number of parameters that need to be defined and tuned to achieve an expected network performance. This paper presents the BAMSim simulator to support the network manager decision process in choosing a set of BAM configuration parameters for network design or during network operation.

1 Introduction

The allocation of resources is an essential aspect in designing existing systems like the internet of things (IoT), smart cities, smart grid, and new generation 5G and 6G systems [5]. Bandwidth is a resource allocated for network substrates that use links between switching nodes to support user communications. Bandwidth allocation is an essential aspect of design in broadly used network infrastructures like multi-protocol label switching (MPLS) network and network infrastructure deployment approaches using OpenFlow/SDN to control level-2 switches or any other switching equipment [4].

The bandwidth allocation models (BAMs) are an alternative to allocate and share bandwidth among network users grouped in traffic classes representing their communication requirements [6]. BAMs are mostly used in networks with limited bandwidth in which there is no over-provisioning for the communication links [11].

This paper presents the BAMSim bandwidth allocation model (BAM) simulator to support the network manager decision process in choosing an appropriate set of BAM configuration parameters during network design and operation.

2 BAMSim Simulator

The BAMSim is specifically oriented to support the allocation of bandwidth on MPLS networks according to the DS-TE (DiffServ Aware - Traffic Engineering) style proposed by Faucher et al. [2]. In summary, the DS-TE style means that bandwidth is allocated by traffic classes (TC), with each TC having a bandwidth constraint (BC).

The BAMSim processes every new LSP demand for the network. The BAM model decides if the LSP is created (allocating bandwidth) or rejected. LSP's requests can be granted, blocked, or preempted depending on the traffic class bandwidth available. Abstractly, an LSP has its starting time, duration, TC, and required bandwidth. The execution module is optionally available to interface the BAMSim simulator with a physical or an emulated network like the MiniNet with OpenFlow-based network control.

BAMSim facilities include: i) The support of MPLS signaling protocol features like LSP establishment, LSP teardown, LSP block and LSP preemption; ii) Network topology definition; iii) Path computation with static matrix and Constrained Shortest Path First (CSPF)

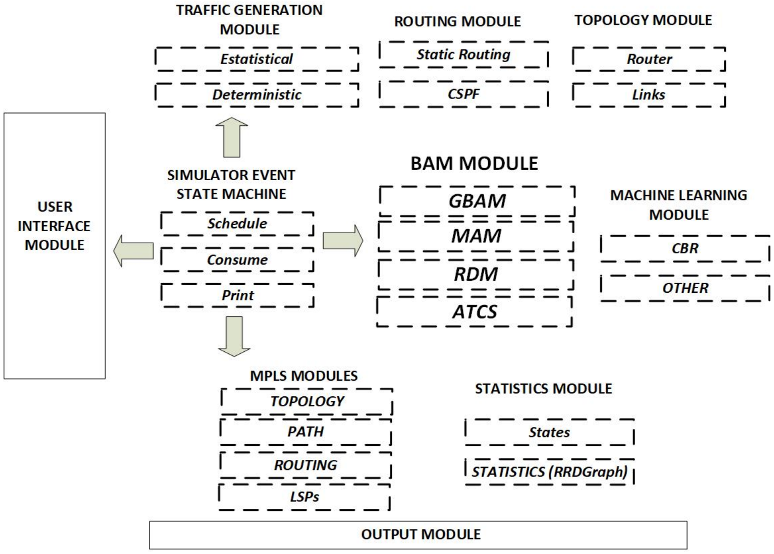


Figure 1: BAMSim Architecture and Internal Modules

route computation; and iv) Input traffic generation (with poisson, exponential and uniform distribution and deterministic traffic).

BAMSim supports the basic BAM models Maximum Allocation Model (MAM) [2], Russian Dolls Model (RDM) [3], and AllocTC-Sharing (ATCS) [10] and the generalized BAM model (GBAM) [8]. The advantages of BAM dynamic model switching and reconfiguration are discussed in [11] [9].

The BAMSim has a modular internal structure implemented in Java. The BAMSim simulator is available at https://github.com/rfreale/BAMSim.

BAMSim related work includes the simulation of BAM models based on the NS (Network Simulator) presented in Adami et al. [1]. The NS module developed simulates MAM and RDM BAM models. Compared with Adami's NS-based module, the BAMSim simulator extends the simulation of BAM modules to all existing models. To the limit of our knowledge, no other BAM simulator as developed since then.

3 BAMSim Architecture and Operation

The BAMSim architecture and main modules are illustrated in Figure 1.

BAMSIM architecture is modular, configurable, and flexible. The simulator code allows the inclusion of functionalities by integrating new modules. The BAMSim allows the configuration of various simulation parameters like simulation time, the simulation runs, number of generated LSPs, LSP duration time, simulation stop conditions, and pseudo-aleatory seeds for traffic generation. BAMSim flexibility includes its capability to import topologies like NSFNet, NTT (Nippon Telegraph and Telephone Corporation), define file-based customized topologies and define routing in the MPLS network with static matrix or protocol computed routing based in protocols like the CSPF.

The MPLS modules abstractly implement the main functions of an MPLS network such as establishment, preemption, devolution, and blocking of LSPs by traffic class (TC) through its interaction with the BAM, topology, path and routing modules in a configurable way.

The BAM module implements the BAM models. A GBAM-based implementation was used in the BAMSim to allow the implementation of all existing BAM models with its operational characteristics and behavior. Another important aspect of using GBAM is that it allows the on-the-fly switching of BAM models to adequate input traffic dynamism, as discussed in [11].

The cognitive module supports the use of machine learning techniques in assisting BAM parameters configuration and BAM model switching according to network traffic and state conditions and according to the objectives defined by the network manager. In the current BAMSim implementation, a Case-based Reasoning (CBR) module is implemented using the jColibri framework [7].

The topology module represents the MPLS network routers and links in an abstract way. The module represents routers interconnection as well as link bandwidth and active traffic classes per link. Topologies can be configured manually or imported by text files.

The routing module enables path selection by integrating a path selection algorithm. The BAMSim can use the CSPF or manually configured path selection algorithms. The routing module is developed in rJava, which allows us to explore the R language resources.

The status and statistics module monitors the states of the network elements and generates statistics and graphics with a Round Robin Database (RRD) using the jRobin library. Statistics are recorded in RRD files since RRD data and charts are intuitive for network managers and used in traditional network monitoring tools.

The traffic generator module allows BAMSim to generate random traffic profiles through probability functions such as uniform, Poisson, exponential, logarithmic, and deterministic traffic for DEBUG and traffic imported from real networks.

4 BAMSim Simulator Application Scenarios

Using BAMSim for BAM-based network design tuning means to evaluate how the configured input traffic impacts the MPLS network performance parameters like LSP preemption, LSP blocking, and link utilization for distinct BAM models. Table 1 illustrates a simulation scenario.

Table 1: Input Traffic - Simulation Pattern Example

Traffic Profile	**1**	**2**	**3**	**4**	**5**	**6**
TC0	High	Medium	Low	High		
TC1	Low	Low	Medium	High		
TC2	Low	High	High	High		
Link utilization	< 90%			>= 90%		

The simulation defines six input traffic profiles with 1 hour each. The first three traffic profile combinations alternate the need for sharing bandwidth between TCs and allows to assess what is the best BAM model option (MAM, RDM or ATCS) for each traffic profile. The last three input traffic profiles force link overload and allow to verify network performance parameters (blocking, preemption, other) and link utilization conditions for distinct BAM models and tune the one that best suits the network manager objectives.

Another BAM-based network-tuning possibility is to reconfigure the traffic class (TC) bandwidth constraints (BC) and, by simulation, to evaluate how the network performance parameters behave for different BAM models.

BAMSim configuration is a straightforward task executed by command line (text file scripts) and GUI-based instructions to the simulator. For example, consider the simulation for a point-to-point MPLS topology with two routers connected by a network link. BAMSim configuration steps include the definition of the network topology (file scripts), input traffic generation characteristics, routing matrix, simulation stop criteria, BAM model and BAM configuration parameters. Script command syntax and semantics are obviously specific to the BAMSim. For example, $PTP - 2n - 1e$ is the topology name with two nodes and one link between routers 0 and 1. Additional syntax and semantics information is available with the BAMSim code.

The BAMSim simulator's utilization to facilitate the learning curve of the BAM configuration process is another relevant application scenario. The BAM teaching simulator's focus is now to allow the modification of the BAM configuration parameters and visualize their effect on the network performance. An application program, based on the BAMSim, was developed with this purpose and is available at https://github.com/rfreale/BAMSim/tree/Education.

5 Final Considerations

The BAMSim, in general, aims to facilitate the design process of bandwidth allocation in network infrastructures and foster the BAM-based bandwidth allocation learning curve. The BAMSim simulator facilitates the manager decision process in choosing the best BAM model and its operating parameters.

References

[1] D. Adami, C. Callegari, S. Giordano, and M. Pagano. A New NS2 Simulation Module for Bandwidth Constraints Models in DS-TE Networks. In *IEEE ICC*, pages 251–255, May 2008.

[2] F L Faucher and W Lai. Maximum Allocation Bandwidth Constraints Model for DiffServ-aware MPLS Traffic Engineering. Technical Report RFC 4125, June 2005.

[3] Le Faucheur, J. Boyle, T. Nadeau, and D. Skalecki. Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering. Technical Report RFC 4127, 2005.

[4] Y. Li, X. Su, A. Ding, A. Lindgren, X. Liu, C. Prehofer, and P. Hui. Enhancing the Internet of Things with Knowledge-Driven Software-Defined Networking Technology. *Sensors*, 20(12), 2020.

[5] Jianhui Liu and Qi Zhang. Computation Resource Allocation for Heterogeneous Time-Critical IoT Services in MEC. *IEEE Wireless Communications and Networking Conference*, February 2020.

[6] Joberto Martins, Romildo Bezerra, Rafael Reale, and Gilvan Durães. Uma Visão Tutorial dos Modelos de Alocação de Banda como Mecanismo de Provisionamento de Recursos em Redes IP/MPLS. *Revista de Sistemas e Computação*, 5(2):144–155, December 2015.

[7] E. Oliveira, R. Reale, and J. Martins. Cognitive Management of Bandwidth Allocation Models with Case-Based Reasoning - Evidences Towards Dynamic BAM Reconfiguration. In *Proceedings of the IEEE Symposium on Computers and Communications*, pages 397–403, June 2018.

[8] Rafael Reale, Romildo Bezerra, and Joberto Martins. G-BAM: A Generalized Bandwidth Allocation Model for IP/MPLS/DS-TE Networks. *International Journal of Computer Information Systems and Industrial Management Applications*, 6:635–643, 2014.

[9] Rafael Reale, Romildo Bezerra, and Joberto S. B. Martins. Applying Autonomy with Bandwidth Allocation Models. *International Journal of Communication Systems*, 29(13):2028–2040, 2016.

[10] Rafael Reale, Walter Neto, and Joberto Martins. AllocTC-sharing: A New Bandwidth Allocation Model for DS-TE Networks. In *Proc. of the 7th Latin American Network Operations and Management Symposium*, pages 1–4, October 2011.

[11] Rafael Freitas Reale, Romildo Martins Bezerra, and Joberto S. B. Martins. Analysis of Bandwidth Allocation Models Reconfiguration Impacts. In *Proceedings of the III International Workshop on ICT Infrastructures and Services (ADVANCE)*, pages 67–76, 2014.

Task Scheduling Model for Fog paradigm

Celestino Barros[1,*], Victor Rocio[2], André Sousa[3] and Hugo Paredes[4]
[1]University of Cabo Verde; celestino.barros@docente.unicv.edu.cv
[2]INESC TEC and Open University of Portugal; vitor.rocio@uab.pt
[3]Critical TechWorks; asousa@roundstone.pt
[4]INESCT TEC and University of Trás-os-Montes and Alto Douro; hparedes@utad.pt

Abstract

Task scheduling in fog paradigm is highly complex and in the literature, there are still few studies. In the cloud architecture, it is widely studied and in many researches, it is approached from the perspective of service providers. Trying to bring innovative contributions in these areas, in this paper, we propose a model to the context-aware task-scheduling problem for fog paradigm. In our proposal, different context parameters are normalized through Min-Max normalization; requisition priorities are defined through the application of the Multiple Linear Regression (MLR) technique and scheduling is performed using Multi-Objective Non-Linear Programming Optimization (MONLIP) technique.

1 Introduction

The growth of mobile devices and the evolution of the Internet of Things (IoT) have stimulated the growth of devices connected to the Internet. This growth tends to increase significantly. On the other hand, several of these devices run applications that requires a part of the processing to run in large, centralized datacenters known as cloud. However, due to centralization and physical distance from end user's devices, it causes an increase in communication latencies and harms applications that require real-time responses. To minimize cloud processing by adopting local processing strategies and allow solving cloud limitations, different techniques have been proposed. One of such technique is the use of the fog computing paradigm [1].

According to [2], many of the task scheduling algorithms in the cloud architecture and fog paradigm found in the literature do not describe how the priority is defined, do not explain the method used to prioritize tasks, nor do they define the prioritization of tasks based on context information, and many defend the perspective of service providers. Others are applied in grouped tasks to decrease execution time. Some optimize only QoS. Others explore only some contexts. The author also claims that they allow solving many problems.

The main objective of this paper is proposing a model of context-aware task scheduling algorithm for the fog-computing paradigm. To achieve its main objective, some specific objectives were defined to contextualize concepts such as fog computing; task scheduling and context-aware; standardize the different context parameters using Min-Max normalization; define the priorities of the requests through the application of the MLR technique and optimize the scheduling using the MONLIP technique.

This paper is organized in four sections: In the first section, we introduce the paper, in the second section we deal with the contextualization of the subject. In the third section, we describe the contexts envisaged, the model and the proposed architecture. In fourth section, we addresses the conclusion of the paper.

2 Background

Mobile computing provides users with several utilities, allows portability, supports applications of various interests, and has several limitations such as scarcity of resources, reduced battery life, among others [2]. In recent years, several architectures have been proposed to solve these limitations, being cloud computing one of them. Despite the advantages, cloud is centralized and for optimization of energy and communications costs, the processing is done in concentrated data centers. To solve these inconveniences, several paradigms have been presented. Among them is fog computing, which aims to make the services offered by the cloud available at the edge of the network [3]. In this section, we contextualize and discuss concepts such as fog computing, context-aware and design of task scheduling algorithms.

2.1 Fog computing

According to [3], fog computing is a new paradigm that aims to overcome the limitations of cloud by providing services at the edge of the network. In [2], it is broadly defined and emphasis is given to some characteristics such as geographical distribution, predominance of wireless access, heterogeneity, distributed environment, among others. As reported in [1], it is: "A horizontal, system-level architecture that distributes computing, storage, control and networking functions closer to the users along a cloud-to-thing continuum."

In the opinion of [4], fog computing from the perspective of mobile computing, aims to provide a cloud-like facility. However, lighter, closer to the users of mobile devices, it can serve these users through direct connection, shorter, compared to the cloud connection.

2.2 Context-aware and fog computing

According to [2], in mobile computing, the context of a user is very dynamic. In [5], a definition, the context categories and context sensitive applications are made available. Information and services, information marking with context and automatic service execution methodology are still presented as well as the survey of the state of the art regarding context-aware computing.

Bazire and Brézillon in [6], define the context as a set of constraints that influence the behavior relating to a given task. The context definition most used today, even in other fields, as in the operationalization was given by [7]:

"Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between user and an application, including the user and applications themselves" [7] (p. 45).

In mobile computing, context refers to the processing environment, user environment, physical environment, relevant for the interaction between a user and an application, including the user and the applications themselves [8].

When mobile devices communicate with cloud, they face high network latency and high transmission power consumption [2]. They also state that in fog paradigm, mobile devices send tasks to fog nodes in order to be processed and returned the result. This process reduces the power consumption of the mobile device, transmission delay, among others. Due to the lower capacity of the fog nodes when compared to cloud, the tasks, which cannot be executed in the fog, are sent to be executed in cloud.

2.3 Design of scheduling algorithms

According to [2], scheduling is the allocation of resources needed to execute a task. In its design, we must consider some constraints such as dependencies between tasks, cost of tasks and the location. It also guarantees that scheduling decisions can be Static - where decisions about scheduling are made during the compilation. On the other hand, it can be dynamic - where information about the state of the task flow is used at a given time during execution for the scheduling decisions. It is the best approach.

However, these problems are computationally demanding, require a strategy of parallelization and dynamic load balancing [2].

3 Proposed model and architecture

We assume that an appropriate code offloading technique (e.g. MAUI defined in [9], COMET presented in [10], among others) is being run on mobile devices in order to make the best decision as to whether or not to offload codes and which fog nodes [11].

We consider that a request includes battery level, QoS information and network signal values. We also assume, as in [4] that fog provides greater computing capabilities than mobile devices and can extract the contexts associated with the requests and make the scheduling decision accordingly.

Musumba and Nyongesa in [8], define the main contexts that can be explored in any mobile computing environment as: network connection; available processors; battery level; location; network bandwidth; network traffic; leased of Virtual Machines (VM) and application QoS requirements.

In our domain of the problem, the contexts of the service providers because we do not know them were ignored. In addition, after offloading the tasks in the fog nodes, it becomes unnecessary to consider the processors of the mobile device. The location of the device also does not affect the scheduling, as well as network traffic and bandwidth that are the same for all users. Based on these criteria we considered three context parameters: battery level, signal-to-noise network interference ratio (SIN) and application QoS.

In the following subsections, we illustrate and discuss the model and architecture of the proposed solution.

3.1 Proposed model

The fog nodes, with our proposal activated, consists of three units: *Context Information Retrieval Unit*, comprises an architecture, as defined in [12]. It retrieves context information (C_i) from each request ($r \in R$). The recovered context information is forwarded to the *Context-Aware Task Prioritization Unit*, which estimates the value of the context priority (P_r) for each individual request $r \in R$ and routes it to the *QoE and Context-Aware Scheduler Unit*, which schedules tasks to be executed in VMs so that QoE is optimized. Figure 1 shows the different units of the proposed model.

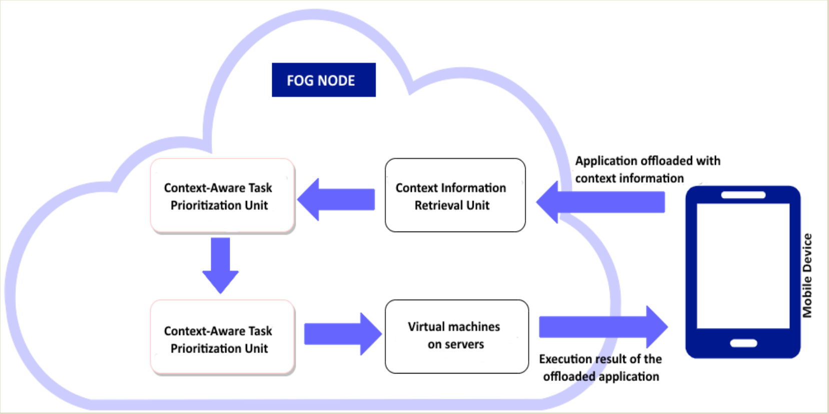

FOG NODE
Context-Aware Task Prioritization Unit
Context Information Retrieval Unit
Application offloaded with context information
Context-Aware Task Prioritization Unit
Virtual machines on servers
Execution result of the offloaded application
Mobile Device

Figure 1: Proposed model.

3.2 Architecture of the proposed model

The fact that the context parameters associated with a request are heterogeneous makes it difficult to explore the context information in the scheduling. To solve this problem, in Han, Kamber and Jian [13], a context heterogeneity resolver is proposed, which processes several parameters, in a normalized interval, through Min-Max normalization, where each request is prioritized based on its context values.

The Context-Aware Task Prioritization Unit is composed by *Context Repository*, which stores context information of current and previously received tasks and *Context Forecasting Unit*, exploits the context information at a given time and feeds the *Forecast Table*. Thus, we manage to eliminate the heterogeneity of the context information in the feeding of the forecast table.

The *Forecast Table* provides a data set for the MLR analysis which aims to define the priority of requests.

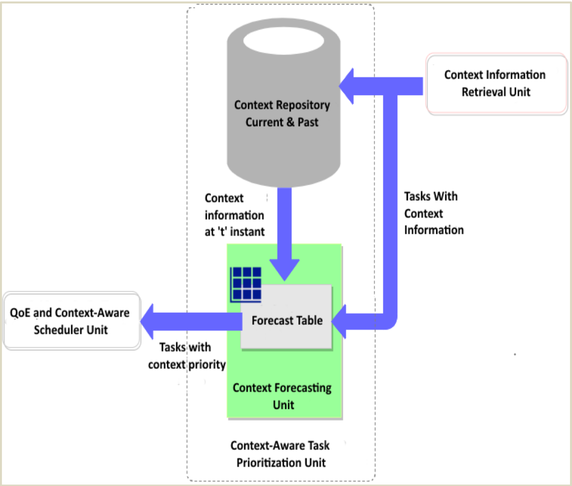


Figure 2: Context-Aware Task Prioritization Unit architecture of the proposed model.

Figure 2 shows the architecture of the Context-Aware Task Prioritization Unit of the proposed model.

3.3 Optimization of application scheduling

In order to optimize QoE, the proposed model explores the context priority (P_r) of the request $r \in R$ and its estimated execution time duration (T_r, v) to define the scheduling of this request $r \in R$ in an VM, $v \in V$. We also explore the number of scheduling intervals (I_r), in which a request is delayed its scheduling since its arrival, in order to avoid the starvation situation.

One of the objectives of this paper consists of scheduling requisitions, $r \in R$ in VM, $v \in V$, in order to optimize the QoE for all the requisitions in a certain scheduling interval.

The OF is defined according to equation 11.

$$\boldsymbol{min_{r,v} \sum_{r \in R} \sum_{v \in V} \frac{P_r * \psi_{r,v}}{I_r}} \tag{1}$$

This equation indicates that the QoE can be optimized by minimizing the sum of their execution times. It also takes into account the priority execution of the tasks with higher priorities by minimizing the sum of the priorities of all requests, since the lower the result, the higher the priority obtained. Moreover, the sum of the inverse values of (I_r), $\forall r \in R$ shows that the requisitions, in which their scheduling has been postponed in a given interval, will have higher priority to be scaled in the current intervals, thus mitigating the starvation situation.

4 Conclusions

The main purpose of this paper of this paper is proposing a model of context-aware task scheduling algorithm for the fog-computing paradigm. To accomplish the main objective, the following piecemeal objectives were achieved:

- We defined some concepts such as fog computing paradigm, context-aware and task scheduling. We intend to contextualize the main theories and concepts related to this paper.
- We propose a model that uses Min-Max normalization, to normalize the different context parameters and solve the problem of heterogeneity of device and application contexts. The MLR analysis was used to define the priority of the context of the requests, which allows the

availability of a set of hypothetical data. The optimal scheduling of requests to optimize QoE was solved by using the MONLP technique.

All proposed objectives were achieved. We consider several context parameters. Others, however, can still be pondered in order to analyze their influences on the scheduling.

Acknowledgments

The authors are grateful to the Calouste Gulbenkian Foundation for its funding of this research through the Ph.D. scholarship under the reference No. 234242, 2019 - Postgraduate Scholarships for students from PALOP and Timor-Leste.

References

[1] OpenFog, "OpenFog Reference Architecture for Fog Computing," *OpenFog*, 2017. https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf (accessed Feb. 24, 2020). URL: https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf.

[2] C. Barros, V. Rocio, A. Sousa, and H. Paredes, "Survey on Job Scheduling in Cloud-Fog Architecture," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 2020, pp. 1–7.

[3] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 1, pp. 50–55, Dec. 2008. DOI: 10.1145/1496091.1496100. URL: https://doi.org/10.1145/1496091.1496100.

[4] T. H. Luan, L. Gao, Z. Li, Y. Xiang, G. We, and L. Sun, "A View of Fog Computing from Networking Perspective," Feb. 2016, [Online]. Available: http://arxiv.org/abs/1602.01509. URL: http://arxiv.org/abs/1602.01509.

[5] A. K. Dey, D. Salber, G. D. Abowd, and M. Futakawa, "The Conference Assistant: combining context-awareness with wearable computing," in *Digest of Papers. Third International Symposium on Wearable Computers*, 1999, pp. 21–28. DOI: 10.1109/ISWC.1999.806639. URL: http://ieeexplore.ieee.org/document/806639/.

[6] M. Bazire and P. Brézillon, "Understanding Context Before Using It," in *Modeling and Using Context*, A. Dey, B. Kokinov, D. Leake, and R. Turner, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 29–40. DOI: 10.1007/11508373_3. URL: http://link.springer.com/10.1007/11508373_3.

[7] A. K. Dey, "Understanding and Using Context, Personal and Ubiquitous Computing, Vol. 5," vol. 5, pp. 4–7, 2001.

[8] G. W. Musumba and H. O. Nyongesa, "Context awareness in mobile computing: A review," *Int. J. Mach. Learn. Appl.*, vol. 2, no. 1, May 2013. DOI: 10.4102/ijmla.v2i1.5. URL: https://ijmla.net/index.php/ijmla/article/view/5.

[9] E. Cuervo *et al.*, "MAUI: Making Smartphones Last Longer with Code Offload," in *Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services*, 2010, pp. 49–62. DOI: 10.1145/1814433.1814441. URL: https://doi.org/10.1145/1814433.1814441.

[10] M. Gordon, D. Jamshidi, S. Mahlke, Z. Mao, and X. Chen, "COMET: code offload by migrating execution transparently," in *Proceedings of the 10th USENIX Conference on Operating Systems Design and Implementation*, 2012, pp. 93–106.

[11] F. Berg, F. Dürr, and K. Rothermel, "Increasing the Efficiency and Responsiveness of Mobile Applications with Preemptable Code Offloading," in *2014 IEEE International Conference on Mobile Services*, 2014, pp. 76–83. DOI: 10.1109/MobServ.2014.20.

[12] H. J. La and S. D. Kim, "A Conceptual Framework for Provisioning Context-aware Mobile Cloud Services," in *2010 IEEE 3rd International Conference on Cloud Computing*, Jul. 2010, pp. 466–473. DOI: 10.1109/CLOUD.2010.78. URL: http://ieeexplore.ieee.org/document/5557960/.

[13] J. Han, M. Kamber, and P. Jian, *Data Mining: Concepts and Techniques*. Elsevier, 2012. DOI: 10.1016/C2009-0-61819-5. URL: https://linkinghub.elsevier.com/retrieve/pii/C20090618195.

SDN Controllers - A Comparative approach to Market Trends

Francisco J. Badaró V. Neto[1,2] , Constantino J. Miguel[1]
Ana Carla dos S. de Jesus[2] , Paulo N.M.Sampaio[1]
Universidade Salvador[1], Centro Universitário UniRuy[2].
fjbvneto@gmail.com, constantino.jacob@gmail.com,
anacarla.dsj@gmail.com , pnms.funchal@gmail.com

Abstract

Software-Defined Networks (SDNs) have been used in the last decade as a solution to provide greater flexibility in controlling traffic being distributed over a network, promoting the reuse and optimization of network resources. SDN´s architecture decouples routing intelligence (Control Plane) from routing functions (Data Plan/Forwarding Plane), through a component called SDN controller which centralizes the Control Plane. Therefore, it is required that the controller´s performance and functions provide an optimal integration with both Forwarding Devices (Network Elements) and with the support to new applications to be proposed within the context of software-defined network paradigm. Nevertheless, the rapid development of this paradigm and the increasing availability of different controllers within the market makes it difficult to choose a suitable one. This paper compares briefly the top six SDN controllers according to the market preference, looking not only to unveil some theoretical aspects but also to have an insight about their market acceptance.

1 Introduction

According to Kreutz et al [1], SDN is an emerging network paradigm that allows to overcome the limitations of current network infrastructures, being defined as a four pillars network architecture: Data and Control Planes are decoupled, the routing decisions are flow-based instead of destination based, the control logics is executed by an external entity called SDN Controller and, the network is programmable through software applications running on the top of the SDN Controller. According to the literature review some efforts were carried out to compare the available SDN Controllers. In [1], Kreutz et al conducted a generalized systematic review of the SDN paradigm and its technological aspects. Nevertheless, this review was not oriented to a comparative study of controllers according to the market perspective. In [4], a systematic review of the SDN controllers and a comparative approach was based on some criteria such as learning curve, supported APIs, documentation availability, Openflow version, among others. Unfortunately, this work does not carry out a comparative classification among the presented controllers and this approach does not focus on the market view perspective, which is important for the acceptance of any technology. At last, Salman et al [3] present a comparison among SDN controllers considering criteria such as programming language, documentation, modularity and performance, also not performing a market-oriented comparison. The main contribution of this paper is the comparative review of the available SDN controllers and their main features, beyond technical and functional perspectives, but also with a market acceptance perspective, documentation availability and OpenFlow support. Therefore, we present a comparative qualitative and quantitative review with a hybrid academic and market perspectives of the top 6 SDN controllers currently available.

2 SDN Controllers

According to Zhu et al [2], an SDN Controller is the core component of any SDN infrastructure, it has the overall network perspective that includes all devices in the data plane. The controller connects these resources with management applications and executes flow control actions dictated by the application policies throughout the devices of the data plane. Figure 1 illustrates the overview of the architecture of an SDN controller and its main components. Other important components in this architecture are the East-West bound interfaces. East-West bound interfaces are also used to communicate with third party APPs and others SDN Controller.

Some important functions in an SDN network operating system are providing abstractions, essential services and providing application programming interfaces to support network programmability. Therefore, being at the top of the control plane, the generic functionalities in an SDN controller can be offered as services such as: network state, network topology information, device discovery and configuration distribution and network actuation/reconfiguration. Some of the main characteristics of SDN Controllers are: (1) *Architecture and Design Axes*, determining a centralized or distributed design providing a higher flexibility and performance to the traffic; (2) *East/Westbound APIs*, which are essential components including functions such as importing and exporting data between controllers, algorithms for data consistency models, monitoring and notification capability, etc.; (3) *Programming languages*, providing interoperability, multithreading, low learning curve, fast access to memory and good memory management are taken into account; (4) *Support to Openflow and other protocols* in the Southbound interface and network programmability.

3 Top 6 SDN Controllers

Classify SDN controllers is a challenge, since there are several criteria that can be applied and some of them are mutually exclusive. Thus, the results of this study aim to support market and academia acceptance of these SDN controllers. Each controller design has a different use case, since their utilization depends not only on their capabilities, but also on the cultural adjustment of the organization and project. In market big picture, according to Bort [5], Cisco incorporated Insieme Networks for $863 million in 2013, with an earlier investment of over $1 billion in the startup, at the time Cisco dominated about 70% of the switch and router market. Cisco, in 2012, had already acquired Cariden Tech for $141 million according to Whittaker [6], thus positioning itself in the SDN market and the new trends in network programmability. Juniper Networks bought Contrail Systems for $176 million in 2012, according to Meyer [7]. An overview could not be made without reporting forecasts on the SDN market. To fill this gap, Dean [8] and Framingham [9], based on the report produced by the International Data Corporation (IDC) about the global SDN market indicates a compound annual growth rate (Compound Annual Growth Rate - CAGR) of 53.9% between 2014 and

2020, which will worth about US$ 12.5 billion in 2020. The following classification was based on the parameters and criteria identified in this study, which consider both technical/academic criteria regarding market criteria indicating the adoption by manufacturers. In addition, based on the SDN Controllers research and classification carried out by Froehlich [10] and IT Central Station [11], the list of 6 top most SDN controllers in evidence in the market is as follows:

6°) HUAWEI AGILE CONTROLLER - Huawey SDN controller, component of its Cloudfabric Solution solutions, Based on ONOS. Strong point is its ability to interoperate with third-party platforms like Vmware vCenter and the broad support for the integration with Openstack platforms, another strength is its support to several protocols for SBI besides Openflow (up to 1.4), such as Restful, Restconf, Webservice, Snmp, OVSDB, JSON-RPC, and sFlow. Due to strict hardware specifications, it requires a large server sizing hardware: CPU 32 cores@2.4 Ghz, 32G memory, 4*1200GB SAS HDD. As a week point, is your large hardware specification.

5º) HP VAN SDN CONTROLLER - HP SDN Controller, also presentes a strict hardware requirements (minimum specifications proposed by HP is 2.2ghz server (intel Xeon or intel Core2 8-core or equivalent)) with 16gb ram and 64gb minimum Storage. Strong points is a very rich API with excellent RSDoc documentation available and a marketplace with several utilities to expand functions via NBI. As a weak point, it only supports Openflow in SBI which greatly limits its applicability.

4º) JUNIPER CONTRAIL - Juniper SDN controller, with end-to-end dynamic configuration and optimization application and control for any cloud infrastructure. Stront points are its extensive documentation, broad support in both SBI and NBI, integration with most cloud services such as the Contrail Cloud service, as well as Kubernets, Openshift and Mesos. It also supports Network Functions Virtualization, A hardware specification with x86 2.2ghz quad-core processor, 12gb RAM, 2 tb HDD meets minimum specifications. As a week point is your high cost.

3º) CISCO ACI (APPLICATION CENTRIC INFRASTRUCTURE) - Cisco SDN Controller, which makes up a set of SDN-applied IP solutions with full native Layer 2-7 integration that supports Vxlan as an extensible overlay/network logic protocol and NFV using GRE (NV-GRE). Strong points are, the extensive case documentation (except for the little NBI documentation) available and a huge marketplace to provide extensions to the controller's native functions via NBI.As a server specification, cloud deployment support (AWS Cloud Support (M5.2x large with Storage Standard S3 Storage and minimum hardware specifications for Baremetal server, 8vCPUs 2.1 Ghz Xeon, 32gb memory, 100gb SSD/300gb . As a weak point is your high cost.

2º) OPENDAYLIGHT SDN CONTROLLER – Linux Foundation's widely used opensource controller, is the basis for several proprietary controllers such as the Ericsson SDN Controller, Fujistu Virtuora, and others. Some of its strengths are its extensive protocol support in SBI as a service abstraction layer with support to a wide range of protocols such as Openflow, OVSDB, NETCONF, BGP, P4, LISP, SNMP, PCEP among others. Some of its weaknesses are the small and outdated documentation of the project on its original website. As for its server specification, 8-cores 64-bit CPU (Intel 64/AMD64) 20gb memory (recommended 3gb memory for each CPU core), 40gb disk.

1º) ONOS SDN CONTROLLER – The Open Network Operating System, is a Linux Foundation project and a leading open source SDN controller for building next generation SDN/NFV solutions and is the basis for several proprietary controllers like Huawei and good market acceptance. As a strength, is the very good documentation and adopt in market. Due to a very rich SBI support to Openflow, P4, NETCONF, TL1, SNMP, BGP, RESTCONF and PCEP protocols, ONOS places itself as one of the controllers with a wider range of SBI coverage. Another great strength is its low hardware requirement: 2x1.8 ghz CPU, 2 GB RAM, 10 GB hdd. For this comparative study, is #1.

4 Conclusions

The comparative study of SDN controllers reveals that there are many options available, between free and proprietary software. The acceptability of SDN controllers was analyzed according to their support to multiple protocols in the SBI, support to different applications at NBI and wide documentation availability. Nonetheless, it is also important to understand the motivations behind the available platforms. Therefore, each designer has different use cases since their utilization depend not only on their functional capabilities, but also on the cultural adequacy of the organization and the project to be applied on. Among the compared SDN controllers ONOS, ODL and CISCO ACI were considered the 3 top-most controllers accepted by the market according to the adopted criteria. Nevertheless, the differences in these criteria from one controller to other criteria can be very subtle, in particular, concerning their technical requirements. For this reason, the adopted criteria were useful to come to a decision. As future work, the context of this article indicates a constant update of the table I due to the dynamic evolution of the related technologies and also of the market oscillations. Opensource projects can oscillate in criteria, requirements and functionalities as well as proprietary designs may also be simply for market reasons, discontinued by their respective owners thus making a classification of SDN controllers beyond a complex task due to the number of possible criteria and the dynamic aspect of these, we can also add the dynamic aspect of the market, which brings this relationship into line with the time of publication and needs to be updated periodically. Also as future work we can include the criterion of adoption of SDN controllers in 5G projects (In Core, Edge, Access/RAN) that size also has the same issues of temporality and technological paradigms mentioned above, as well as the fact that, would lead to a greatly increased ratio of controllers, changing the comparative context from TOP 6 to TOP 10.

5 References

[1] KREUTZ, D. et al. Software-Defined Networking: A Comprehensive Survey. Oct. 2014. Available at: https://arxiv.org/pdf/1406.0440.pdf Accessed on 01/26/2021.

[2] ZHU, L. et al. SDN Controllers: Benchmarking & Performance Evaluation. Feb. 2019. Available at: https://arxiv.org/pdf/1902.04491.pdf . Accessed on 01/26/2021.

[3] SALMAN, O. et al. SDN Controllers: A Comparative Study. Abr. 2016. Available at: https://www.researchgate.net/publication/304457462_SDN_controllers_A_comparative_study Accessed on 04/13/2020.

[4] GONÇALO, J.S.P. , SOUSA, P. A comparative study of software defined networking (SDN) controllers (in portuguese). June. 2019. ISBN: 978-989-98434-9-3.

[5] BORT, J. Cisco Launches Its Secret Startup Insieme, Then Buys It For $863 Million. 6 nov. 2013, Business Insider. Available at: https://www.businessinsider.com/cisco-buys-insieme-for-863-million2013-11 . Accessed on: 01/26/2021

[6] WHITTAKER, Z. Cisco buys network traffic software firm Cariden Tech for $141m. 29 nov. 2012, ZDNet. Available on: https://www.zdnet.com/article/cisco-buys-network-traffic-softwarefirm-cariden-tech-for-141m Accessed on: 01/26/2021.

[7] MEYER, D. Juniper buys enterprise SDN firm Contrail for $176m. 13 dez. 2012, ZDNet. Available at: https://www.zdnet.com/article/juniper-buysenterprise-sdn-firm-contrail-for-176m Accessed on: 01/26/2021.

[8] DEAN, S. 5 Open Source Software Defined Networking Projects to Know. 7 fev. 2017, LiNUX.com. Available at: https://www.linux.com/news/open-cloud-report/2016/5-open-sourcesoftware-defined-networking-projects-know Accessed on 01/26/2021.

[9] FRAMINGHAM, M. SDN Market to Experience Strong Growth Over Next Several Years, According to IDC. 3 fev. 2016, Business Wire. Available at: https://www.businesswire.com/news/home/20160203005954/en/SDN-Market-Experience-Strong-Growth-Years-IDC . Accessed on 01/26/2021.

[10] FROEHLICH, A. 10 SDN Platform Options. 9 mar. 2016, Network
Computing. Available at: https://www.networkcomputing.com/networking/10-sdn-platform-options Accessed on 01/26/2021.

[11] IT Central Station. Best Software Defined Networking (SDN) Solutions. Apr. 2019.
Available at: https://www.itcentralstation.com/categories/software-defined-networking-sdn Accessed on 01/26/2021.

Blockchain Applications with Permissioned Distributed Ledger Technology

Alan Nascimento Gomes[1] and Emanuel Ferreira Coutinho[1]

Federal University of Ceara (UFC), Quixadá, Ceará, Brazil
alanng@alu.ufc.br,emanuel.coutinho@ufc.br

Abstract

Blockchain is currently a technology that has been attracting a lot of attention both in academia and industry. Several areas of expertise are benefiting from blockchain due to its characteristics, such as data security, decentralization, traceability and immutability. The objective of this work is to present the use of a blockchain allowed with the implementation of a prototype in the context of e-health applications. Preliminary results indicate that blockchain can be well used for e-health applications, integrating with other technologies.

1 Introduction

Blockchain is a technology that is currently increasingly strengthening as a distributed database technology, becoming widespread both in academia and in industry. With the popularization of the digital currency Bitcoin proposed by Satoshi Nakamoto [8], several sectors became target of research for the insertion of this technology in applications that need characteristics, such as: decentralization, reliability, traceability and immutability [12].

Blockchain technology is a decentralized network (P2P) that has its own layer of protocol messages for node communication. Transactions stored on the network are encrypted and stored in blocks. Each block has a reference to the previous block, which allows a temporal ordering of transactions [5]. According to the use and development of blockchains networks in different fields, two types of blockchains have arisen that are used according to the needs of each application, which are: Permissionless Blockchains (public), characterized by the permission that is given to any network participant to read or send transactions, and Permissioned Blockchains, which are characterized by the need that the nodes have to be accepted in the network to carry out operations. This last type of blockchain is used when data preservation is necessary, such as in the health sector [1].

In literature, several articles have dedicated themselves to implementing solutions using blockchain technology [7] [6]. In [7], the authors proposed the permissioned blockchain platform Hyperledger Fabric for the safe and reliable sharing of electronic patient records. As a result of the proposed work, it was shown that Hyperledger removes the lack of trust between health centers, doctors, public health departments and hospitals. The authors of [6] focused on allowing an increase in the degree of confidence patient health data. This solution was proposed through an architectural solution based on blockchain for granting permission to access health data obtained from a Patient Monitoring System (SMRP).

E-health has increasingly explored the monitoring technologies to improve the efficiency of healthcare professionals in treating patient [9]. The objective of this work is to present the use of applications with permissioned blockchains, in the context of e-health domain, and present an experiment that uses the Hyperledger Fabric blockchain platform [3].

This work is divided into the following sections: Section 2 presents the methodology and design of the experiment; in Section 3, the results are shown; and finally, in Section 4 the conclusion is presented.

2 Methodology and Design of Experiment

In 2015, a collaborative project of the Linux Foundation emerged that aims to develop several open source frameworks and tools for permissioned blockchains in a modular way, called Hyperledger. The use of permissioned DLTs (Distributed Ledger Technology), such as Hyperledger, is justified by the need that solutions require some features, such as: data security, faster transactions and reliable network of participants. Notable cases of these applications are: supply chain, property registration and patents [4].

Hyperledger Fabric is one of the technologies of Hyperledger. In this technology, it is possible to implement a modular and pluggable architecture in which it allows the use of several programming languages for the implementation of smart contracts used by applications. With Fabric, it is also possible for a network to contain chains of isolated blocks that allow the partition of different participants and executable codes for smart contracts [10].

Smart contracts, in Fabric called chaincodes, are executable codes, invoked by a client application outside the network, responsible for leveraging blockchain technology. They are a collection of code and data deployed using cryptographically signed transactions on the blockchain network [2] [13].

In this work, smart contracts (chaincodes) are used to perform operations of insertion and reading of information in a Hyperledger Fabric network. This information is related to the identification of patients. The application that interacts with the blockchain network has the responsibility to collect data that comes from patients and store it on the network, simulating the creation of an electronic medical record. With this action, it is possible that the information will become practically immutable and used in audits, provided that access to this data is requested and authorized.

The use of blockchain technology in applications like these allows the monitoring of the history of medical visits, the study of the development of diseases and even the assessment of people's quality of life, as it facilitates the management of consultations in health institutions [11].

For this article, the prototype of an application that inserts data from a patient into the Hyperledger network was implemented, with the purpose of simulating the registration of electronic medical records. In this application, it is possible to carry out transactions responsible for the registration of a new patient, recovery of all registered patients and the search for the history of medical records by the patient ID.

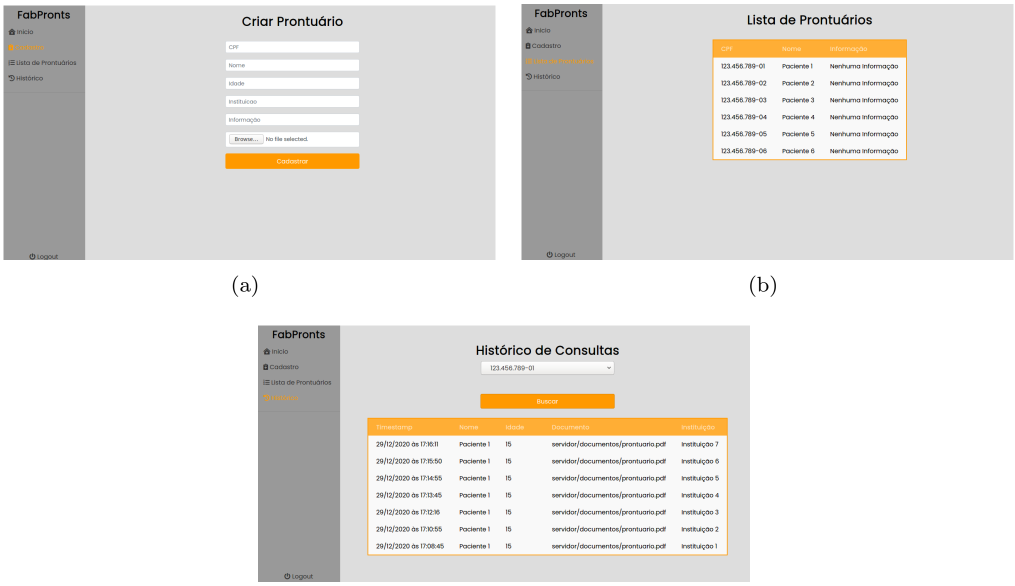
3 Results

In this section, the results of the application prototype mentioned above will be presented.

In Figure 1, it is possible to analyze the application prototype. In Figure 1(a), the fields that collect the patient's data are presented, which are: ID (acting as the key of the transaction), Name, Age, Institution (represents the health institution in which the patient is visiting), Information; Document (this field makes it possible to upload a file to complement the medical record information, only the link to that file will be stored on the network).

Figure 1(b) shows a list of patients that are stored in the Hyperledger network. Even if there is more than one registration with the same ID, the search for a transaction will return the data informed in the last transaction of the searched key.

Figure 1(c) shows the transaction history. For this function, the Hyperledger network returns, linked to each transaction, a value called timestamp that indicates the time stamp in which that transaction occurred. Through this feature it is possible to obtain a patient's history



(a)

Lista de Prontuários

CPF	Nome	Informação
123.456.789-01	Paciente 1	Nenhuma Informação
123.456.789-02	Paciente 2	Nenhuma Informação
123.456.789-03	Paciente 3	Nenhuma Informação
123.456.789-04	Paciente 4	Nenhuma Informação
123.456.789-05	Paciente 5	Nenhuma Informação
123.456.789-06	Paciente 6	Nenhuma Informação

(b)

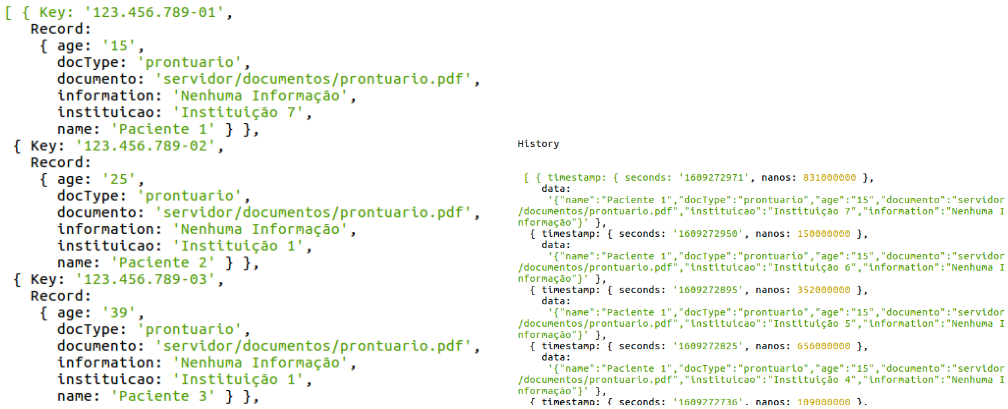
Histórico de Consultas

123.456.789-01

Timestamp	Nome	Idade	Documento	Instituição
29/12/2020 às 17:16:11	Paciente 1	15	servidor/documentos/prontuario.pdf	Instituição 7
29/12/2020 às 17:15:50	Paciente 1	15	servidor/documentos/prontuario.pdf	Instituição 6
29/12/2020 às 17:14:55	Paciente 1	15	servidor/documentos/prontuario.pdf	Instituição 5
29/12/2020 às 17:13:45	Paciente 1	15	servidor/documentos/prontuario.pdf	Instituição 4
29/12/2020 às 17:12:16	Paciente 1	15	servidor/documentos/prontuario.pdf	Instituição 3
29/12/2020 às 17:10:55	Paciente 1	15	servidor/documentos/prontuario.pdf	Instituição 2
29/12/2020 às 17:08:45	Paciente 1	15	servidor/documentos/prontuario.pdf	Instituição 1

(c)

Figure 1: Application screens (in brazilian portuguese)



```
[ { Key: '123.456.789-01',
    Record:
     { age: '15',
       docType: 'prontuario',
       documento: 'servidor/documentos/prontuario.pdf',
       information: 'Nenhuma Informação',
       instituicao: 'Instituição 7',
       name: 'Paciente 1' } },
  { Key: '123.456.789-02',
    Record:
     { age: '25',
       docType: 'prontuario',
       documento: 'servidor/documentos/prontuario.pdf',
       information: 'Nenhuma Informação',
       instituicao: 'Instituição 1',
       name: 'Paciente 2' } },
  { Key: '123.456.789-03',
    Record:
     { age: '39',
       docType: 'prontuario',
       documento: 'servidor/documentos/prontuario.pdf',
       information: 'Nenhuma Informação',
       instituicao: 'Instituição 1',
       name: 'Paciente 3' } },
```

(a)

```
History


 [ { timestamp: { seconds: '1609272971', nanos: 831000000 },
     data:
      '{"name":"Paciente 1","docType":"prontuario","age":"15","documento":"servidor
/documentos/prontuario.pdf","instituicao":"Instituição 7","information":"Nenhuma I
nformação"}' },
  { timestamp: { seconds: '1609272950', nanos: 150000000 },
     data:
      '{"name":"Paciente 1","docType":"prontuario","age":"15","documento":"servidor
/documentos/prontuario.pdf","instituicao":"Instituição 6","information":"Nenhuma I
nformação"}' },
  { timestamp: { seconds: '1609272895', nanos: 352000000 },
     data:
      '{"name":"Paciente 1","docType":"prontuario","age":"15","documento":"servidor
/documentos/prontuario.pdf","instituicao":"Instituição 5","information":"Nenhuma I
nformação"}' },
  { timestamp: { seconds: '1609272825', nanos: 656000000 },
     data:
      '{"name":"Paciente 1","docType":"prontuario","age":"15","documento":"servidor
/documentos/prontuario.pdf","instituicao":"Instituição 4","information":"Nenhuma I
nformação"}' },
  { timestamp: { seconds: '1609272736', nanos: 109000000 },
```

(b)

Figure 2: Data returned from the Hyperledger Fabric network

by searching for the key. In Figure 1(c), transactions with time marks are shown for the patient with ID 123.456.789-01.

All three operations carried out with the network discussed in the previous paragraphs were done by executing chaincode executable codes, implemented in the javascript language.

Figure 2 presents the return obtained after the execution of the operations with the network. In Figure 2(a), part of the network response is shown when a request is made to list all transfers and in the Figure 2(b), the answer that contains the history of the patient whose ID is 123.456.789-01.

4 Conclusion

This work presented the use of a permissioned blockchain through an application prototype that performs the registration of electronic medical records. The focus of the prototype was to use the Hyperledger Fabric platform to track medical visits by patients in healthcare institutions. This research is at an early stage, but preliminary results indicate that blockchain can be well used for e-health applications, integrating with other technologies.

This work collaborates with the disclosure of permissioned blockchains and their applications. As future work, it is planned to complete the implementation of the application and verify the performance of the network with different workloads.

Acknowledgments: This work was supported by PIBIC 2020/2021 (01/2020) program, project **Integração de Aplicações E-health com Ambientes de Computação em Nuvem e Blockchain**, from Federal University of Ceará (UFC).

References

[1] H. Desai, M. Kantarcioglu, and L. Kagal. A hybrid blockchain architecture for privacy-enabled and accountable auctions. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 34–43, 2019.

[2] Hyperledger Fabric. Glossary, 2020. https://hyperledger-fabric.readthedocs.io/en/release-2.2/glossary.html.

[3] Hyperledger Fabric. Hyperledger fabric model, 2020. https://hyperledger-fabric.readthedocs.io/en/release-2.2/.

[4] Daniel Duarte Figueiredo. Fundamentos em blockchain. 2020.

[5] Florian Glaser. Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis. 2017.

[6] Natália Junqueira, Gabriel Silva, and Sergio Carvalho. Concessão de permissão a dados de saúde baseada em blockchain. 2019.

[7] N. Kumar S. and M. Dakshayini. Secure sharing of health data using hyperledger fabric based on blockchain technology. In *2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI)*, pages 1–5, 2020.

[8] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008. Online; acessado em fevereiro-2019.

[9] M. M. Neto, E. F. Coutinho, L. O. Moreira, J. N. de Souza, and N. Agoulmine. A proposal for monitoring people of health risk group using iot technologies. In *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–6, Sep. 2018.

[10] Gabriel Antonio F Rebello, Gustavo F Camilo, Leonardo GC Silva, Lucas Airam C de Souza, Lucas CB Guimarães, Eduardo AP Alchieri, Fabíola Greve, and Otto Carlos MB Duarte. Correntes de blocos: Algoritmos de consenso e implementação na plataforma hyperledger fabric. In *38o Jornada de Atualização em Informática (JAI) do XXXIX Congresso da Sociedade Brasileira de Computação (CSBC 2019)*, 2019.

[11] Caroline Viana, Alexandre Brandão, Diego Dias, Gabriela Castellano, and Marcelo de Paiva Guimarães. Blockchain para gerenciamento de prontuários eletrônicos. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E28):177–187, 2020.

[12] G. Wang, Z. Shi, M. Nixon, and S. Han. Chainsplitter: Towards blockchain-based industrial iot architecture for supporting hierarchical storage. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 166–175, 2019.

[13] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. Blockchain technology overview. *arXiv preprint arXiv:1906.11078*, 2019.