ADVANCE'2019

7th International Workshop on ADVANCEs in ICT Infrastructures and Services

January 21th-22th 2019, Praia, Cape Verde

Faculdade de Ciências e Tecnologias" of the University of Cape Verde (UNICV)

978-2-9561128-2-2 9782956112822

Edited by Mr. Tamazirt Lotfi

Preface

The 7^{th} International Workshop on ADVANCEs in ICT INfrastructures and Services (ADVANCE 2019), held between January 21-22, 2019 in Santiago Island, Cape Verde.

The focus of this workshop is once again to sustain the important efforts of the worldwide scientific community, practitioners, researchers, engineers from both academia and industry to have a forum for discussion and technical presentations on latest theoretical and technological advances in ICT to solve societal challenges for developed and under developing countries. The workshop aims to develop the link between scientists from academia and industry worldwide to fade the digital divide between countries and organisation allowing all of them to access to the latest knowledge and collaborate together.

After the successful organization of the 1st ADVANCE workshop in 2012 in Canoa Quebrada (Brazil) with the support of IFCE Aracati, the 2nd edition 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) and finally, this 7th edition will be held in the Cape Verde Islands with the support of the Universidade de Cabo Verde making the link between the three continents (South America, Africa and Europe).

Advances in technologies such as IoT, Big Data, Blockchain, among others, have put enormous challenges on communication infrastructures and IT services. In this sense, ICT technologies as a whole, must be able to follow this evolution and promote solution that meet these ongoing challenges. Since these solutions would enable interaction not only between things, but also between thing and man, we need to analyse and discuss how these technologies impact our lives.. The Advance workshop is a unique venue where all these aspects have been discussed between the participating researchers and industrials within the various technical sessions. Technical session have addressed several technical challenges that have impact in various society domains such as health, transportation, energy and so on.

The proceedings of the ADVANCE '2019 contains all the papers presented during this edition. Among 18 papers submitted, 8 papers have been accepted as full papers and 9 as work in progress papers. The technical programme included 3 invited talks from Mr Antonio Fernandes (PCA Nosi, Cape Verde), Prof Hakim Abdelhafid (University of Montreal, Canada) and Dr Isaías Barreto da Rosa (Chairman Multisectoral Regulatory Agency of the Economy (ARME), Cape Verde) about respectively Certification of the ICT Development in Cape Verde, Blockchain - opportunities and limitations and The role of ICT in promoting economic development, government transparency and fighting in Africa.

We take here the opportunity to thank all the members of the ADVANCE 2019 technical program committee as well as the reviewers. The proposed technical program of the workshop would not have been possible without their commitment and efforts. We also gratefully thank all the authors that dedicated much of their time and efforts to contribute to this workshop. We also kindly thank the members of the ADVANCE 2019 organizing committee for their help in handling the logistics of the event. Finally, we would like to acknowledge the support of the University of Cabo Verde and the coordination of the Computer Engineering course in the successful organisation of this workshop in Cape Verde.

We would like also to thank EasyChair organisation for providing us with their valuable service.

January 21-22, 2019
Praia, Cape Verde

Prof Claudino Mendes, CVU, Cape Verde
Prof Jose De Souza, UFC, Brazil

Program Committee

Wassila Aggoune-Mtalaa	Luxembourg Institute of Science and Technology, Luxembourg
Nazim Agoulmine	IBISC/University of Evry - Paris Saclay University, France
Mustapha Ait-Idir	Banque du Canada, Canada
Mehdi Ammi	LIMSI-CNRS, France
Rossana Andrade	Federal University of Ceará - UFC, Brazil
Javier Baliosian	Universidad
Djamel Belaïd	Institut Mines-Telecom, Telecom SudParis, France
Sonia Ben Rejeb	Sup'com, Tunisia
Reinaldo Bezerra Braga	LAR / Federal Institute of Technology in Ceará - IFCE, Brazil
Karima Boudaoud	CNRS I3S - University of Nice Sophia Antipolis, France
José Bringel Filho	State University of Piauí - UESPI, Brazil
Joaquim Celestino Jr	Universidade Estadual do Ceará - UECE, Brazil
Olfa Chabbouh	Sup'com, Tunisia
Tijani Chahed	Institut Mines-Telecom, Telecom SudParis, France
Elhadi Cherkaoui	Beamap, France
Emanuel Coutinho	Federal University of Ceara - UFC, Brazil
Paulo Cunha	Federal University of Pernambuco - UFPE, Brazil
Carlos A.B De Carvalho	Federal University of Piaui, Brazil
César Olavo De Moura Filho	Instituto Federal de Educaçao, Ciencia e Tecnologia , Brazil
Neuman Desouza	Federal University of Ceará - UFC, Brazil
Elias Duarte	Federal University of Parana, Brazil
Ahmed Elmisery	Federico Santa María Technical University
Alilat Farid	University of Sciences - USTHB, Algéria
Miguel Franklin De Castro	Federal University of Ceará - UFC, Brazil
Danielo Gomes	Federal University of Ceará - UFC, Brazil
Hanna Klaudel	IBISC, university of Evry, France
Sergio Manuel Serra Da Cruz	UFRRJ, Brazil
Joberto Martins	Salvador University - UNIFACS, Brazil
Claudino Mendes	Universidade de Cabo Verde - UCV, Cabo Verde
Thiago Moreira Da Costa	IBISC/University of Evry - Paris Saclay University, France
Jonice Oliveira	Universidade Federal do Rio de Janeiro - UFRJ, Brazil
Paulo Sampaio	Universidade Salvador - UNIFACS, Brazil
Marcelo Santos	Federal Institute Sertão-PE., Brazil
Abderrahim Sekkaki	Faculty of science, Hassan II University, Casablanca, Morocco
Flavio Semedo	Universidade de Cabo Verde, Cabo Verde
Carina Teixeira De Oliveira	Federal Institute of Ceará (IFCE), Brazil
Rafael Tolosana	Universidad
Arlindo Veiga	Universidade de Cabo Verde, Cabo Verde
Augusto Venâncio Neto	Universidade Federal do Rio Grande do Norte - UFRN, Brazil

Author Index

Table of Contents

Keyword Index

Full Papers

A Blockchain-based Educational Record Repository

Emanuel E. Bessa[1*] and Joberto S. B. Martins[2†]

[1] Salvador University, Salvador, Bahia, Brazil
emanuel.bessa@hotmail.com
[2] Salvador University, Salvador, Bahia, Brazil
joberto.martins@unifacs.br

Abstract

The Blockchain technology was initially adopted to implement various cryptocurrencies. Currently, Blockchain is foreseen as a general purpose technology with a huge potential in many areas. Blockchain-based applications have inherent characteristics like authenticity, immutability and consensus. Beyond that, records stored on Blockchain ledger can be accessed any time and from any location. Blockchain has a great potential for managing and maintaining educational records. This paper presents a Blockchain-based Educational Record Repository (BcER^2) that manages and distributes educational assets for academic and industry professionals. The BcER^2 system allows educational records like e-diplomas and e-certificates to be securely and seamless transferred, shared and distributed by parties.

1 Introduction

Blockchain is a technology considered by many to be something as relevant as the rise of the Internet. There have been experiments with blockchains since the early 1990's, but it was only in 2008, with the release of a white paper by an individual or group of individuals under the pseudonym of Satoshi Nakamoto, that blockchains gained wide adoption [9].

The first well-known blockchain-based implementation was the cryptocurrency Bitcoin [9]. Bitcoin is also the first widely-used, decentralized cryptocurrency. Basically, Blockchain technology is a shared peer-to-peer distributed ledger implementing a distributed database with some security characteristics.

Blockchain is a technology that may potentially support application development in many distinct areas. It is a peer-to-peer transaction management system without an intermediary. Blockchain allows transactions to be verified by a network of nodes and recorded in a public distributed ledger [2].

Educational records are used worldwide and, from the user point of view, is an important asset for individuals pledging for scholarships, jobs and professional and academic visibility in general.

In the educational context, a "certificate" is a type of educational record that represents an educational achievement or some type of relevant membership. University degrees, course and conference registers can eventually help individuals to get the job they want. In case you do not have a valid certificate, this may potentially prevent individuals from getting it. Currently, our educational records management systems are mostly physically localized, require specific and non-trivial procedures to access information, are in many cases unreliable and, finally, do not follow or have any educational standards.

Communication is currently available on a worldwide basis potentially allowing wide spread interactions and fostering visibility for citizens on various scenarios.

[*] Bessa, E. is with UNIFACS IPQoS research group

[†] Prof. Dr. Martins, J. is with UNIFACS IPQoS and NUPERC research groups

With the blockchain capabilities and citizen's global visibility perspective in mind this paper presents a Blockchain-based Educational Records Repository (BcER^2). BcER^2 is intended to allow any individual to be able to store educational records and access multiple type of educational records with authenticity on a worldwide basis. It is a system to ensure educational records distributed management and access with inherent more security like authenticity and privacy.

This study focuses on the viability and benefits of Blockchain applied to the field of formal and non-formal education. In this way, Blockchain also represents an opportunity for the public to independently and privately verify that shared records are authentic and unadulterated.

In the next part of this article, section 2 summarizes the fundamental aspects of Blockchain technology. Section 3 indicates the relevant work being done related to Blockchain and BcER^2 system. Section 4 describes the architecture, entities, components and implementation of the BcER^2 system. Section 5 presents a proof-of-concept of the BcER^2 implementation. Finally, section 6 presents the final considerations and future work.

2 Fundamental aspects of Blockchain Technology

A blockchain is essentially a distributed database of records that keeps potentially all kind of data, like transactions, contracts and events. All information handling takes place across a peer-to-peer network and is maintained chronologically in digital blocks. These basic features and capabilities make Blockchain transparent, secure, decentralized and with almost unlimited storage capacity[4].

Chained blocks keep the history of all transactions made by the users since they access the system. As such, Blockchain can be also described as a register on which everyone can write, but cannot erase and/or destroy. As a result of using a peer-to-peer network, all copies of the records can be shared between the various computers known as ”network nodes”, consequently decentralizing the network and eliminating intermediaries.

Blockchain uses the concept of hashing. The ”hash” is a block signature and considers all data and transactions involved. In summary, a cryptography hash function takes a input string and turns it into a unique n-digit string [9]. Figure 1 illustrates how blocks are chained in Blockchain.

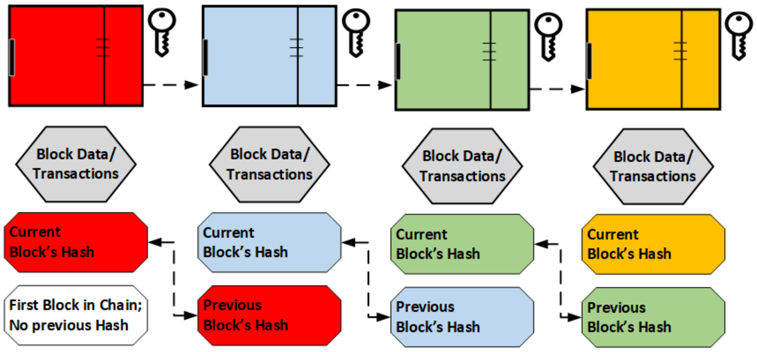


Figure 1: Blockchain basic operation

2.1 Key Blockchain Characteristics

With traditional methods for recording transactions and tracking assets, participants on a network keep their own ledgers and other records. This traditional method can be expensive, partially because it involves intermediaries that charge fees for their services. It's clearly inefficient due to delays in executing agreements and the duplication of effort required to maintain numerous ledgers. It's also vulnerable because if a central system (for example, a bank) is compromised due to fraud, cyberattack, or a simple mistake, the entire business network is affected. To solve or improve traditional method Blockchain has a set of key characteristics: consensus, provenance, immutability and finality [9] [2].

All relevant participants make decisions by consensus, in this process most participants must agree that a transaction is valid. This goal is achieved through the implementation of consensus algorithms. Each network enforces the conditions under which transactions are performed or the exchange of assets may occur. Provenance guarantees that participants know where the asset came from and how its ownership has changed over time. With immutability, no participant can tamper with a transaction after it has been recorded to the ledger. If a transaction is in error, a new transaction must be used to reverse the error, and both transactions are then visible. With finality, a single shared ledger provides one place to go to determine the ownership of an asset or the completion of a transaction.

2.2 Why ”Blockchain” to Manage and Improve Visibility for Educational Records

An “education record” in the context of this paper is a record containing files, documents, and other materials which [9]: i) Contains information directly related to the academic historical of a student or a professional; and ii) From a local perspective are typically maintained by an educational institution or by other entity acting for such institution.

There are significant advantages and benefits in using a Blockchain-based educational repository [3] [17]: i) Educational records (e-diplomas, e-certificates, other) uploaded and managed on the Blockchain ledger are more secure and resistant to “physical wear and tear” than paper documents [3]; ii) Educational records are seamless and efficiently transferred and shared among parties (universities, schools and employers) fostering worldwide visibility; and iii) Educational records stored on the blockchain can be accessed any time, from any location.

In summary, educational records managed by Blockchain technology stimulate the knowledge/reward principle, makes credentials more trustworthy and keeps educational records safe and easy to access [3].

3 Related Work

In recent years, blockchain technology has been widely used as the basic construc for cryptocoins such as Bitcoin [15]. For some experts this is considered the first generation of Blockchain. The use of Blockchain in this sense has grown considerably and it is currently estimated that there are over 1600 crypto-coins. [15].

MIT has a system for building Blockchain-based applications that issues and verifies official records called ”Blockcerts Wallet”. It allows, for instance, the creation of a certificate wallet for students to receive virtual diplomas via their smart devices [13]. Differing from Blockchain-based Educational Records Repository (BcER^2), MIT Blockcerts Wallet system is a building application platform that have a similar target in terms of allowing educational records creation and dissemination using Blockchain.

New promisingly Blockchain-based solutions include ’intelligent contracts’ [14] . Ethereum, discussed in [16], allows the creation of contracts that are self-managed. Contracts are triggered by an event such as passing an expiration date or achieving a specific price goal. In response, the smart contract manages itself by making adjustments as needed and without the input of external entities [1]. Blockchain utilization for automated smart contracts dealing with energy transactions for the Smart Grid is discussed in [14].

As time went on and the hype of the cryptocurrencies passed, developers began to realize that Blockchain could do more than simply manage ’document transactions’. Jurdak et al. in [6] discusses Blockchain adoption for privacy and security support in the Internet of Things (IoT). Blockchain cybersecurity and privacy performance vis-a-vis cloud solutions is discussed in [11]. Barguil et al. in [5] discuss how blockchain technology and smart contracts can improve data access, data management and data interoperability of Electronic Health Records (EHR). Potential Blockchain application towards innovation in Smart Cities are discussed in [7]. Blockchain applications for supply-chain to validate individuals and assets are introduced in [10]. A mobile edge computing enabled Blockchain system is presented in [18] to allow its application in mobile services where computational capability is limited.

Blockchain deployment may have problems like scalability and required processing power [19] [6]. Some of the effort made by researchers and developers in the area will be in solving scalability and processing capability problems, thereby giving more applicability to Blockchain technology.

4 The Blockchain-based Educational Records Repository (BcER^2) - Architecture and Components

In order to meet the different alternatives of use, blockchain-based applications can be implemented using 3 types of general structures as follows [2]: i) Public Blockchain; ii) Private Blockchain; and iii) Consortium Blockchain.

The type of Blockchain structure to be used strongly depends on the application. The BcER^2 repository adopted the consortium system since only authorized persons are able to create certificates records on the network. On the other hand, anyone can verify their authenticity. Thus, when registering an educational record, for example, the responsible for creating the record writes in the registry or in the database using its own private key. Users who want to check the veracity of the record must have a corresponding identifier number to be inserted into the system.

The public Blockchain arose from the need for a totally decentralized blockchain structure that allows open use, reading and participation in the management of operations within the network. The main feature of this model is the secure protection of users.

The private Blockchain owns its business network written and developed by a centralized organization. The company writes and verifies each transaction, in addition to deciding the network read permissions. This increases efficiency, enhances user confidentiality, and reduces transaction costs. All the autonomy on the part of the organization constitutes its main characteristic.

The Blockchain consortium is a semi-private and partially decentralized chain system, in this scenario the nodes are responsible for the validation of the transactions and how this happens depends on the implementation of the consensus methods. The form of access and consultation of the records can be public or private and the owner of the network is responsible for its configuration.

The BcER^2 effective structure uses the basic steps and operation flow of a blockchain-based application as illustrated in Figure 2: i) A transaction is requested by someone who has prior authorization and needs to create an educational record; ii) The request record transaction is sent to the nodes belonging to the BcER^2 system; iii) The educational record transaction is verified by the ledger; and iv) A new block of data corresponding to the educational record transaction is accessed or created and annexed to the ledger becoming permanent and immutable completing the transaction.

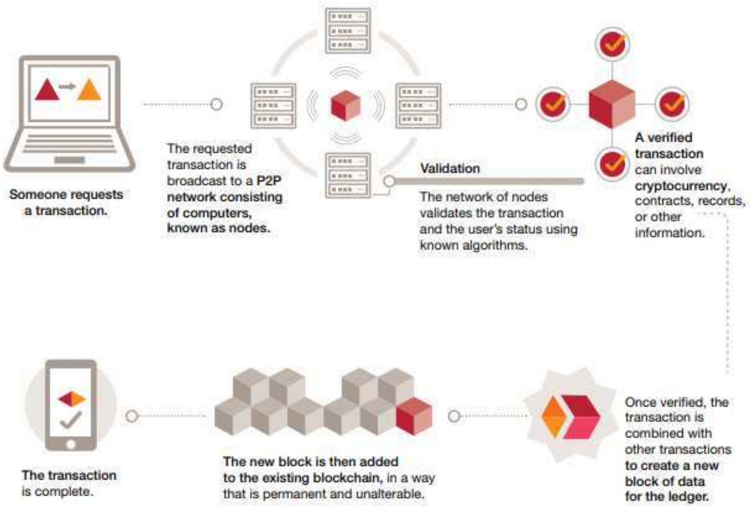

Someone requests a transaction.
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.

Figure 2: BcER^2 basic steps and flow operation - Figure available at [2]

4.1 Blockchain-based Educational Records Repository (BcER^2) Entities

The entities belonging to the BcER^2 educational repository are the following: i) Assets; ii) Registers; iii) Transactions; and iv) Participants.

An ”asset” can be anything of value that will be kept securely by the educational repository. Educational records like certificates, diplomas, educational records an similar documents are BcER^2 assets.

”Participants” are the educational organization representatives, students and people in general that are somehow interested in either distributing or accessing educational records. Participants are defined in the ”business network model” adopted by the blockchain application process. For BcER^2, coordinators, students, and anyone else interested in having access to the educational records are the participants belonging to the network. Each one has their specifically assigned functions, responsibilities and access restrictions.

”Transactions” are submitted by participants to create or access the assets held in the blockchain-based asset registries on the blockchain ledger. Transactions, in general, do belong to a business network and, as such, do require a ”business network model”. The business network model, from the blockchain system perspective, define the operation involved with the

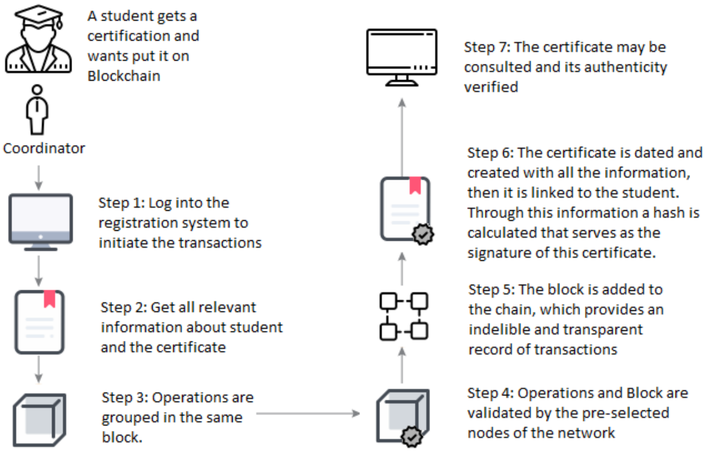

A student gets a certification and wants put it on Blockchain
Coordinator
Step 1: Log into the registration system to initiate the transactions
Step 2: Get all relevant information about student and the certificate
Step 3: Operations are grouped in the same block.
Step 4: Operations and Block are validated by the pre-selected nodes of the network
Step 5: The block is added to the chain, which provides an indelible and transparent record of transactions
Step 6: The certificate is dated and created with all the information, then it is linked to the student. Through this information a hash is calculated that serves as the signature of this certificate.
Step 7: The certificate may be consulted and its authenticity verified

Figure 3: ”Certificate Register” creation in BcER^2

assets.

”Registers” can be defined as the set of data that involve the assets, transactions and the participants. this set is what will be included in the block after the validation. Registers are new information that is added to the blockchain ledger.

In BcER^2 educational records repository the addition of a ”register” is carried out through the execution of steps. In these steps, the business model adopts the following ”business” premises: i) The course coordinator or the educational institution representative are the authority to create new assets; and ii) Students and general public are participants that access the validated and secure educational assets maintained by the system.

The creation of a register is executed as illustrated in Figure 3: i) A coordinator proceeds to write a record to the Blockchain account, which means create the certificate with an identifier. In this process the coordinator selects the certificate and through its identifier number it is possible to link it to a student; ii) The revcord is saved and time-stamped in a block using arithmetic operations; iii) The block is subsequently validated by network pre-selected nodes through cryptography techniques; and iv) The block is dated and added to the block chain, so that all users can have access to the same chain since each node builds its own exemplary independently.

Once these steps have been executed, we can access educational records with authenticity and integrity by simply using a credential (ID Card) through a web browser.

4.2 Blockchain-based Educational Records Repository (BcER^2) Business Network

The business network is a fundamental definition for the BcER^2 educational registry repository deployment.

In summary, it models the BcER^2 ”educational model”, defining the existing assets, transactions and participants related to them. The business network defines the transactions that interact with assets. The model also includes the definition of participants who interact with assets and associates a unique identity, across multiple business networks. As described before, BcER^2 is composed of assets, participants and transactions, with each of these entities modeled in relation to the educational operation.

4.3 Blockchain-based Educational Records Repository (BcER^2) Components

The basic components belonging to the the BcER^2 educational records repository are illustrated in Figure 4 and basically reflect the business network adopted which is suitable for an educational records repository that registers, manages and provide access to them.

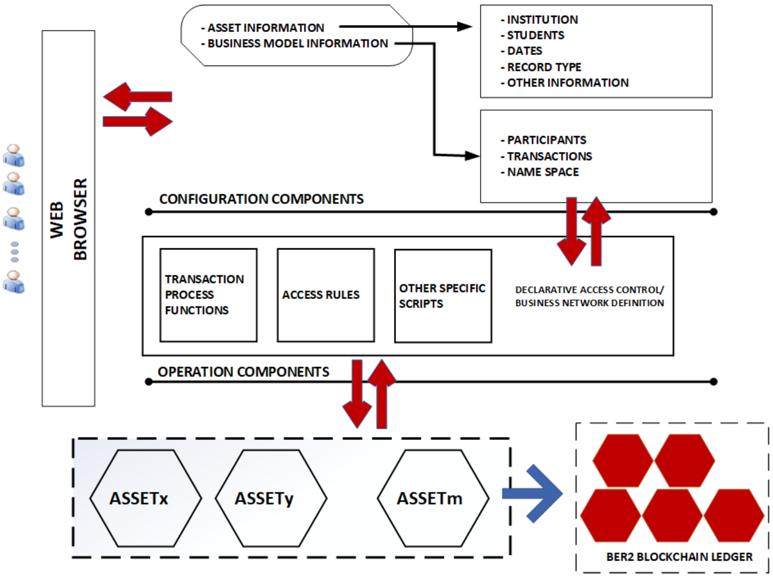


Figure 4: BcER^2 basic components

The "asset information" component contains information related to the educational record being managed by BcER^2. This component is responsible for asset's definition and consistency.

The "Business Model Information" component contains information related to the process involved in the asset management. It defines basically the participants, name space and transactions involved in the process.

The "Transaction Process Function" component contains the information concerning the specif functions invoke in the business model to manage the asset.

The "Access Rules" component contains, as the name suggests, the access rules including all priorities among participants involved in the business model adopted.

BcER^2 managers and general users access the repository through a web browser using identification cards (ID Cards) which includes connection profiles and credentials.

Assets are effectively deployed in the BcER^2 blockchain ledger in this specif system by the Hyperledger Composer framework described in section 4.4.

4.4 Blockchain-based Educational Records Repository (BcER^2) Implementation

The Hyperledger Composer [8] was used to implement the BcER^2 educational repository (Figure 5). Hyperledger Composer is an open source development tool set and framework aiming to support the development of blockchain applications. It allows the modeling of the business network and integrates existing systems components and data deploying as such the blockchain application.

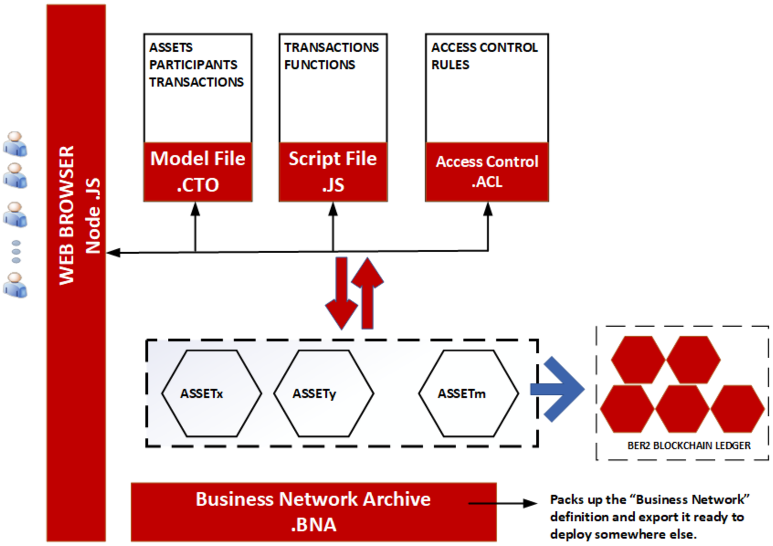


Figure 5: Hyperledger Composer deployment

The use case adopted by the actual implementation is initially intended to verify the authenticity of student's certificates generated by Salvador University (UNIFACS) under-graduation courses.

BcER^2 is composed of assets, participants and transactions, with each of these entities being represented within Hyperledger framework as configuration files ((Figure 5).

The .CTO hyperledger component is responsible for implementing the assets, participants, and transactions, including all relevant information. A Hyperledger Composer CTO file is composed of the following elements: i) A name-space with resources declaration; ii) Resources definition including assets, transactions, participants and events; and iii) Optional resource import declarations from other name-spaces.

The .ACL hyperledger component provides declarative access control for the elements in the domain model. By defining access and control (ACL) rules you can determine which users/roles are permitted to create, read, update or delete elements in a business network's domain model.

The 'Business Network' definition, from the Hyperledger Composer perspective, is composed by a set of model files defining assets, participants and transactions (Figure 5). The ".JS" script file is responsible for maintain a set of scripts. The scripts contain transaction process functions that implement the transactions defined in the 'Business Model'. Transaction processing functions are automatically invoked at run-time when transactions are submitted and their structure are composed by a JavaScript function.

5 BcER^2 Repository - Proof-of-Concept

The main objective of the BcER^2 repository proof-of-concept is to validate the deployment of the business network and verify the operation steps of the repository by: i) Creating assets;

and ii) Accessing them and verifying the effectiveness of credentials and other distribution and security aspects.

The proof-of-concept of the BcER^2 repository operation was implemented by emulating participants as follows: i) 'Users' are the general public accessing educational records; and ii) The 'Coordinator' (Register Authority) is a UNIFACS authority creating educational record entries.

The experiment was executed using the following infrastructure: i) The BcER^2 system runs on Notebook Core i7, 2.0 Ghz, 8 GB RAM, Ubuntu Server Operating System 16.04 x64; and ii) The coordinator and users access the BcER^2 system using any browser.

The software components installed to run the BcER^2 system are i) Node Version 8.12; ii) NPM Version 6.4.1; iii) Visual Studio Code Version Version 1.28; iv) Docker Engine Version 18.06; and v) Docker Composer Version 1.23.

The proof-of-concept method and parameters used to validate the operation of BcER^2 was the creation of a set of educational records followed by authenticity verification and access by the system administrator and distributed users. The experimental setup included the creation of 10 different educational records with course certificates and various nodes (N>10) simulating different users acting on the validation process (transactions) and verifying their authenticity. The results allowed the distributed access to educational records enabling verification through blockchain technology. Security access was also validated by trying to access educational records without the adequate credential. The scalability of the solution was not evaluated and will be addressed by future work.

6 Final Considerations and Future Work

New technologies have always attracted companies and governments. This is largely due to the promise to improve the current way of working and providing services. Blockchain technology is a new strategy that gives users great possibilities of use. This technology has demonstrated great potential with the possibility of eliminating intermediaries, besides having great advantages such as security, transparency and confidentiality of the users. This is offered by a database similar to a registry, implemented in a shared way between all nodes in a network. Most experts agree with its potential and Blockchain technology is being applied and new use cases are being implemented every day.

We propose in this work to use Blockchain technology as a tool to provide a secure and efficient way to access certificate with authenticity. We argue that the proposed Blockchain BcER^2 repository has the potential to support the education sector by providing better support for certificate management and distribution.

In the current scenario, the proposed application covers only the UNIFACS network for the purpose of managing diplomas and certificates issued by the university. The BcER^2 application has the potential to cover additional areas in which digital certificates provide interesting opportunities such as [12]: i) Corporate Training - Many large companies offer a multitude of training opportunities to their employees, but lack the systems to track and store results reliably. Current human resources systems often do not interact with corporate databases and there are no consistent standards for comparing skills and accomplishments; and ii) Workforce Development - There are millions of records and learning certificates, but there are no systems to manage them. This is especially a problem for people with low qualifications, who often do not have recognized diplomas or degrees.

In terms of future work, it is intended to evaluate the scalability issues and impacts associated with the deployment of a huge repository. Another aspect to be considered is to bring together stakeholders such as employers, students, teachers and contractors in a way that they interact with each other enabling wide-spread use of trustable e-certificates. A final target will be to adopt a fully standardized asset representation as an additional step towards a secure and decentralized way of conferring a wide-spread use of the system.

7 Acknowledgements

Authors thanks FAPESB (Fundação de Apoio à Pesquisa do Estado da Bahia) by the scientific initiation (IC) scholarship support.

References

[1] Habib Azam. *What are the different generations of blockchains?* Jan. 2018. URL: https://medium.com/@habs/what-are-the-different-generations-of-blockchains-bebf3c3ad57f (visited on 11/16/2018).

[2] Sanjaya Baru. “Blockchain: The next innovation to make our cities smarter”. en. In: (Jan. 2018), p. 48. URL: https://www.pwc.in/publications/2018/blockchain-the-next-innovation-to-make-our-cities-smarter.html.

[3] Institute of Blockchain^{TM}. *Blockchain and Education.* June 2018.

[4] Michael Crosby. “BlockChain Technology: Beyond Bitcoin”. In: 2 (2016), p. 16.

[5] Arlindo F. da Conceição, Flavio S. Correa da Silva, Vladimir Rocha, Angela Locoro, and João Marcos M. Barguil. “Eletronic Health Records Using Blockchain Technology”. In: *Anais Do I Workshop Em Blockchain: Teoria, Tecnologias e Aplicações - WBlockchain - SBRC 2018.* Vol. 1. SBC - Brazilian Computer Society, May 2018.

[6] Ali Dorri, Salil S. Kanhere, and Raja Jurdak. “Towards an Optimized BlockChain for IoT”. In: *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation.* IoTDI ’17. New York, NY, USA: ACM, 2017, pp. 173–178. ISBN: 978-1-4503-4966-6. DOI: 10.1145/3054977.3055003.

[7] FICCI and PwC India. *Blockchain: The Next Innovation to Make Our Cities Smarter.* https://smartnet.niua.org/content/d18d3972-ff71-4ce8-af03-6079f1849bd5. 2018.

[8] Linux Foundation. *Introduction — Hyperledger Composer.* URL: https://hyperledger.github.io/composer/latest/introduction/introduction (visited on 11/16/2018).

[9] Alexander Grech and Antony F. Camilleri. *Blockchain in Education.* Tech. rep. EUR 28778 EN. Luxembourg: European Union, 2017, pp. 1–136. DOI: 10.2760/60649.

[10] Nir Kshetri. “Blockchain’s Roles in Meeting Key Supply Chain Management Objectives”. In: *International Journal of Information Management* 39 (Apr. 2018), pp. 80–89. ISSN: 0268-4012. DOI: 10.1016/j.ijinfomgt.2017.12.005.

[11] Nir Kshetri. “Blockchain’s Roles in Strengthening Cybersecurity and Protecting Privacy”. In: *Telecommunications Policy.* Celebrating 40 Years of Telecommunications Policy – A Retrospective and Prospective View 41.10 (Nov. 2017), pp. 1027–1038. ISSN: 0308-5961. DOI: 10.1016/j.telpol.2017.09.003.

[12] MIT Media Lab. *Certificates, Reputation, and the Blockchain.* Oct. 2015. URL: https://medium.com/mit-media-lab/certificates-reputation-and-the-blockchain-aee03622426f (visited on 11/16/2018).

[13] MIT Media Lab. *What we learned from designing an academic certificates system on the blockchain*. June 2016. URL: https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196 (visited on 11/16/2018).

[14] M. Mylrea and S. N. G. Gourisetti. "Blockchain for Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security". In: *2017 Resilience Week (RWS)*. Sept. 2017, pp. 18–23. DOI: 10.1109/RWEEK.2017.8088642.

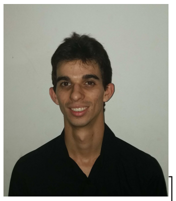
[15] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". In: (2008), p. 9.

[16] Nathan Reiff. *Blockchain Technology's Three Generations*. en. July 2018. URL: https://www.investopedia.com/tech/blockchain-technologys-three-generations/ (visited on 11/16/2018).

[17] Raza Sheeraz. *Blockchain Can Help People Keep Their Educational Records Intact*. en-US. May 2018.

[18] Zehui Xiong, Yang Zhang, Dusit Niyato, Ping Wang, and Zhu Han. "When Mobile Blockchain Meets Edge Computing". en. In: *arXiv:1711.05938 [cs]* (Nov. 2017). arXiv: 1711.05938 [cs].

[19] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. "Where Is Current Research on Blockchain Technology?—A Systematic Review". en. In: *PLOS ONE* 11.10 (Oct. 2016), e0163477. ISSN: 1932-6203. DOI: 10.1371/journal.pone.0163477.



] Emanuel E. Bessa - Computer science student at Salvador University (UNIFACS). Research interest include Blockchain technology and Smart Cities. Emanuel is a member of IPQoS Research Group and RePAF Project (Resource Allocation Framework for MPLS, Elastic Optical Networks (EON), Network Function Virtualization (NFV) and IoT) at UNIFACS.

] Prof. Dr. Joberto S. B. Martins - PhD in Computer Science at Université Pierre et Marie Curie – UPMC, Paris (1986), PosDoc at ICSI/ Berkeley University (1995) and PosDoc Senior Researcher at Paris Saclay University – France (2016). Invited Professor at HTW – Hochschule für Techknik und Wirtschaft des Saarlandes (Germany) (since 2004) and Université d'Evry (France). Full Professor at Salvador University on Computer Science, Head of NUPERC and IPQoS research groups with research interests on Cognitive Management, Artificial Intelligence, Resource Allocation, SDN/ OpenFlow, Internet of Things, Smart Grid and Smart Cities. Senior member of IEEE Smart Grid and IEEE Smart City Research Committees and former Chair of the IEEE CGAA (Committee on Global Accreditation Activities).

A secure and smart environment for the transportation of dangerous goods by using Blockchain and IoT devices

Adnan Imeri[1,2], Nazim Agoulmine[2], and Djamel Khadraoui[1]

[1] Luxembourg Institute of Science and Technology
adnan.imeri@list.lu
[2] Universitè of Èvry Val d'Essonne - Paris Saclay University
nazim.agoulmine@univ-evry.fr

Abstract

The impact of the Internet of things (IoT) attributes for a better quality of services in several domains also in transportation. The information generated from IoT devices is essential for daily activity in the domain of transportation. For the transport activities related to dangerous goods, the information shared and exchanged by stakeholders of the supply chain for dangerous goods is considered sensitive and should be protected from the access of unauthorized parties. This paper intends to show the potential of blockchain technology for securing information generated by IoT devices in the context of transportation of dangerous goods.

1 Introduction

In recent years, we witness many changes in the technology domain, which has shaped the current way of performing business processes. The new emerging technologies such as the Internet of Things (IoT) enables redesigning of the new business process. The Internet of Things (IoT) is composed set of devices which are connected for a specific scenario, and they exchange particular information [11]. These devices enable emerging of many technological concepts, such as Smart Manufacturing, Smart City, Smart Home, Smart Offices, etc. [9] [21]. The usability of these technologies, accompanied with particular devices allows better management of enterprise activities, by allowing them to monitor active processes they are performing. The new emerging concepts such as Industry 4.0, intends to transform the way of managing manufacturing, management of logistics and transportation [15]. While the urban activities are growing, there is an implication on increasing services for daily activities. These services may come from the perspective of transportation and other activities which are related to transportation. The use of IoT devices in such environment shows many potentials on better management of service related to transportation, better public information, security, and monitoring for any public activity, thus decreasing challenges in case of accidents. One of the main concerns remains on the privacy and security of information generated by IoT devices [19][33][7]. Through this research paper, we intend to show the potential of blockchain technology for securing the information generated by use of IoT devices in the monitoring the process of transportation of dangerous goods, by approaching a potential real case in Luxembourg.

1.1 Transportation of Dangerous Goods (TDG)

Dangerous goods (DG) are defined as substances which exposes a high risk for humans, living organisms, environment and property. The evaluation of risk exposed by TDG is an challenging task presented by scientific literature [12] [10] [20] [30]. The DG varieties in different classes such as "Explosives", "Gases", "Solids", "Oxidizing materials", "Flammable Liquid", "Radioactive

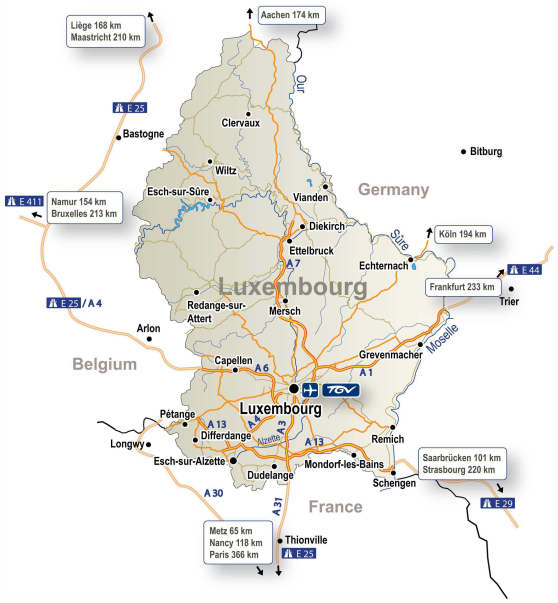


Figure 1: The map of the route network in Luxembourg. Image Copyright SIP [5]

.

materials, "Corrosive substances", "Miscellaneous" [28]. The DG present a high risk during the transportation process. The challenge originates from the fact that the accidents of anywhere a subject are DG have catastrophically consequence [29]. The significant percentage of TDG is performed every day [27]. A notable presence in transportation statistics is allocated for the TDG, and the transportation network comprises a large number of DG daily [13]. The governance of this process is subject of predefined national and international regulation which determine a sustainable process for TDG. These regulations intend of minimizing the risk by standardizing the process of TDG [17]. The research from [28] elaborates the procedures for packing, labeling, loading, transporting, unloading and warehousing of dangerous goods.

1.2 Challenges regarding TDG in Luxembourg

The TDG involves several challenges because of specificity of the goods which are transporting. The possible accidents with DG demonstrate a high risk for population, private and public properties, and environment since the transportation network usually overpasses urban areas. Following we present the use case of Luxembourg transportation network, that is usually used from other neighbor countries, as a hub for the transportation of goods. Since the most suitable way for TDG is by using roads due to the low costs, compared to other means of transport, the shipping (transport) organization intends to select the shortest route possible to minimize the costs. That exposes a problem, while the transportation network passes through a populated area [27]. This challenge is related to Luxembourg scenario, where main roads move nearby to the populated area, as presented in Figure 1. The highways and local roads, most of the time are massively overloaded with many traffic congestion, and that increases the risk of accidents with DG. For example, the highway (number A31), is massively used by trucks as transit highway for the cross into other neighbor states such as France, Germany, Belgium, and Netherlands.

1.3 The decision support systems as a management tool for TDG

The risk involved in TDG comes from the nature of goods which are subject to transportation. For the risk estimation and management of the processes of TDG, there are designed and develop decision support systems (DSS) as a computer-based solution. The basic idea behind DSS is to help stakeholders to measure the risk for TDG, to save time on critical decision, monitoring the process of transportation [27], decrease the negative impact in case of accidents with dangerous goods [36], scheduling, planning and resource allocation [23][14] [27] [23]. In general, the architecture of these systems is composed of several other systems. The embedded systems for "Sensors", "GPS tracker", "RFID", "GIS for moving objects", and other related ones, which are integrated into the main architecture of DSS, provides information for the process of TDG. The risk analysis, monitoring of the process of TDG and other related tasks are depended on the current state of information which should be provided by these systems. For example, in case of an accident in the process of TDG, the IoT devices (GPS tracker, Sensors, RFID, Raspberry Pi) would provide information regarding this accident in the real time. The information regarding the process of TDG, managed by DSS are stored in the local database of the stakeholders. This exposes several concerns due to the security of information, reliability, and trust issues regarding the process of TDG by other stakeholders or authorities, and we will discuss it on the section below.

1.4 The concern of information security in TDG

The use of IoT devices significantly improves the quality of the process for TDG by advancing the monitoring and reaction in case of abnormal situations, i.e., accidents or other distribution on the process of TDG. The concern of using the IoT devices remains on the security of information exchanged by the IoT devices in the process of TDG [19][33][7]. The current DSS systems are mainly centralized or partly hosted in cloud [7], they remain the only point of reference for data exchange. The IoT frameworks such as Amazon Web Services (AWS) [4], Salesforce [1], does not guarantee the data immutability since they are hosted in the facilities of cloud providers. This way of organizing the storage and management of IoT data does not fulfill the security requirements for the process of TDG.

For the context of TDG, where "nuclear materials or nuclear waste" might be among transporting substance", the security, confidentiality, auditing, and monitoring or processes in real time are extremely recommended. In the line of concerns, the following question raises *"Why we need to secure the information captured from the IoT Devices ?"*.

Since the process of TDG is mostly an international activity, that crosses borders of countries whose stakeholders are involved. For this process, a different international and local regulatory frameworks are applied, and usually, the stakeholders involved are the ones with big market reputation [17]. In case of any accident or irregular process in TDG, the secured information captured from the IoT devices are currently not immutable, and this allows big market players to impact the process by changing the information. The design of current technologies which support the storage of IoT data does not guarantee this level of data security. For ensuring such a system, an extended answer for the following question should be provided:

- Remove the single point of failure in such systems?

- How to secure the information generated by IoT devices?

- How to secure the information provided by stakeholders, e.g., exchange of documents by stakeholders of DG?

- The TDG operations and the process should be auditable?

The primary intention behind this conceptual research is the security of information in the top of DSS or other IoT cloud solutions. For achieving this, we propose a conceptual, described in section 3

2 Related works study: Blockchain and IoT

Blockchain is a distributed database which allows storing of the immutable transaction. The transactions in blockchain might contain financial information, trade information, etc.[32]. The blockchain network is composed of several nodes which communicate with each other in a peer to peer mode. All the nodes included in the blockchain network contain the same ledger, and they relay their communication in each other instead of any central authority [35]. The blockchain nodes gather transaction into ”blocks”, performs cryptographic check (public-private key cryptography), and seek to add them to the chain of blocks. The process of adding a new block into blockchain is called ”mining”, and the nodes which perform this mining is called miner. The miner proposes a new block after achieving a consensus challenges set by consensus protocol. The block of transactions which are stored into blockchain are immutable, and cryptography tools ensure data integrity [32]. The fundamental characteristic of blockchain is that the block of data is linked together, so the block N contains the hash address of previous block N-1 [22] [32]. The tendency for changing the information stored into blockchain is denied by consensus protocol e.g., Proof of Work, or Proof of Stake, etc., which verifies the state of data [31].

Smart Contracts: A computer code which is deployed into blockchain and triggered when certain conditions are fulfilled. The smart contracts are self-executed programs for fulfilling given task [2]. An example of smart contract execution is presented for the case of temperature parameters that possibly overcome the fixed level.

IoT devices: RFID, Sensors, GPS tracker, and RaspberyPi, are among IoT devices which are intended to be used for conceptualizing our approach. We will use RFID to store some information about DG. Then, for measurement of temperature, humidity, and abnormal disturbance we will use sensors. GPS tracker devices monitor the location of goods. A more advanced device such as Raspberry will be used to sign transactions.

The scientific community shows many efforts on settling up the new emerging technologies together, blockchain and IoT. A Survey research for the integration of blockchain and IoT is showed in [24], while the challenges and opportunities of integrating blockchain are studied by [25]. A new data transfer layout for IoT based on blockchain technology called IOTA is presented in [3]. The research from [18] presents different architectural styles for using IoT and blockchain. [26] found that the blockchain technology has attractive properties for decentralizing the IoT, thus proposing an architecture for integration blockchain and IoT. The new way of controlling and configuring IoT devices by storing the private key into the device and public key into blockchain nodes [16]. The research from [8] showed that blockchain and smart contract in combination with IoT device, have a significant impact on the automation of processes.

3 Smart and secure environment for TDG

Our conceptual approach intends to change the trend of managing the TDG in line with the security of information. We intend to develop a new way of storing information by using blockchain technology.

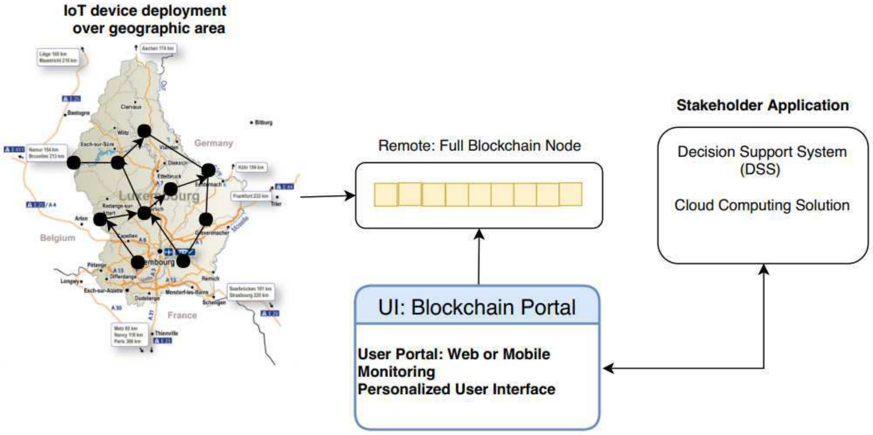


Figure 2: The conceptual approach for smart and secure TDG supply chain

We propose a decentralized solution based on IoT device and blockchain technology. A smart and secure environment in the context of TDG which expect to respond the security concerns presented section 1.4. The sketch from Figure 2, presents the conceptual solution for a smart and secure environment for TDG.

The core of our solution is composed of three main components. The first one represents the IoT devices. The second component is blockchain technology, and the third one is the stakeholder's side, the DSS or any other cloud solution.

For composing the conceptual approach, we deploy the IoT devices over the geographic area and also into transport mechanisms such as trucks. First, these IoT devices are registered on the blockchain, by using their hardware identification [16]. This registration allows them to store their private key in their memory. That avoids receiving information from an unauthorized IoT device. These IoT devices are known as blockchain lightweight node[1], which means that they don't contain complete blockchain, but they use their memory and processing capacity to sign transaction [6]. Second, when the transaction is signed, the IoT device sends this transaction into "Remote Full Blockchain Node", which collect transaction from all IoT nodes and verifies them. There are several mining nodes in our system. For the verification of the transaction, this node checks if the received transactions are from registered IoT device. Further, these nodes add a new block into blockchain. Third, when the block has been added into the blockchain, the *smart contracts* are triggered to fulfill their conditions, in case any parameter is reached, e.g., the high level of temperature on the truck for TDG. Fourth, all stakeholders involved in this process can insert a set of immutable information by using "blockchain portal[2]", for the purpose of the process of TDG, and further, they can monitor the whole process for TDG.

For example, in the context of TDG, the stakeholders initiate this procedure by exchanging information. In our conceptual solution, they can do this by using *"blockchain portal"*. These set of parameter, like the type of goods, itinerary, specific information about DG, e.g., temperature, disturbance, etc., are inserted related to the TDG. Then during the process of transportation, the IoT device detects these goods when reaching its area of detection. The IoT devices receive information regarding the current state of the goods and sign this information by forming a transaction which further will be transmitted into blockchain. The stakeholders and other

[1] The Full Node and Lightweight Node: https://www.mycryptopedia.com/full-node-lightweight-node/

[2] The combination of IPFS and blockchain: https://ipfs.io/

authorized parties can monitor all operations in TDG by using *”blockchain portal”*.
In such an approach, even if some nodes fail to respond, still the system can provide information since the blockchain distributes information in all nodes. The information captured from IoT devices are signed cryptographically and sent to full blockchain nodes making this information immutable. The user interface allows users to provide their data on the blockchain-based system. The ability of immutable record keeping of blockchain enables a full audition of processes and operations for TDG.

4 Technological alignments with business requirements for TDG

The focus behind the proposed conceptual solution for the smart and secure environment for TDG is smart contracts. Various smart contracts are proposed for fulfilling the requirements for the proposed system. Following we detail one of the significant smart contracts:

AlertSC which alerts stakeholders in case of an emergency, i.e., the high temperature of goods. This smart contract is deployed in ”Full Blockchain Node” in our solution. It waits without any action until receiving any parameter for triggering it. A simple structure of for this smart contract is expressed below:

```
S0: parameters: stakeholderList, IoTDeviceList, SubstanceList,
     transportedSubstance, location, timestamp, riskLevel, TempLevelSubstance
S1: check (if ReceivedTransaction in IoTDeviceList)
S2: check (if transportedSubstance in SubstanceList) and
           (TempLevelSubstance >=substanceRiskLevel)
S3: check (if stakeholder in stakeholderList)
S4: function (sendMessage: Alert (location, timestamp) -> stakeholder))
```

Along with possibilities offered by the blockchain technology, numerous challenges emerging while aligning business process requirements with the technology features. Mainly the source of these challenges is the insufficient maturity of blockchain technology to respond to all possible business requirements emerged from the business process. The alignment of business requirements rise challenges on the expression of smart contracts. For example, in the context of our study, the legal regulation should be considered in TDG. The expression of legal rules into smart contract arise a research challenges. Further, the performance issue of the blockchain is among the cancers from the scientific community [34]. The main concern in this scenario is the scalability. Regarding this concern in our proposed scenario, while the number of transaction received from IoT devices might be increasing daily in line with transport activity, the current blockchain ability might face difficulty to respond them in real time. Encountering, then the alignment of the business process requirements and the scalability issues we intend to extend our research by implementing the proposed conceptual approach and providing empirical analysis regarding the behavior of the entire system.

5 Conclusion and Future Works

In this paper, we propose a new way of securing information in the process of TDG by combining the IoT devices with blockchain technology. We performed a potential real case scenario, along with it we intend to develop that as proof of concepts in the near future. This approach promises on overcoming of several challenges in the management of process for TDG. Furthermore, we identified some challenges which stem from combining the IoT devices with blockchain technology. These challenges are on scalability and the alignment of regulatory framework with blockchain technology.

References

[1] Crm software & cloud computing solutions - salesforce emea. https://www.salesforce.com/eu/?ir=1. (Accessed on 11/12/2018).

[2] Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. (Accessed on 11/14/2018).

[3] iota1_4_3.pdf. https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf. (Accessed on 11/16/2018).

[4] Machine learning at aws. https://aws.amazon.com/machine-learning/. (Accessed on 11/12/2018).

[5] Road network - luxembourg. http://luxembourg.public.lu/en/cartes-du-luxembourg/05-reseau-routier/index.html. (Accessed on 12/21/2018).

[6] whitepaperanyledger.pdf. http://www.anyledger.io/whitepaperAnyLedger.pdf. (Accessed on 11/13/2018).

[7] Mahmoud Ammar, Giovanni Russello, and Bruno Crispo. Internet of things: A survey on the security of iot frameworks. *Journal of Information Security and Applications*, 38:8–27, 2018.

[8] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. *Ieee Access*, 4:2292–2303, 2016.

[9] Annalisa Cocchia. Smart and digital city: A systematic literature review. In *Smart city*, pages 13–43. Springer, 2014.

[10] Andrea Conca, Chiara Ridella, and Enrico Sapori. A risk assessment for road transportation of dangerous goods: a routing solution. *Transportation Research Procedia*, 14:2890–2899, 2016.

[11] Li Da Xu, Wu He, and Shancang Li. Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, 10(4):2233–2243, 2014.

[12] Lianhong Ding, Yifan Chen, and Juntao Li. Monitoring dangerous goods in container yard using the internet of things. *Scientific Programming*, 2016, 2016.

[13] Eurostat. Road freight transport by type of goods - statistics explained. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Road_freight_transport_by_type_of_goods#Road_freight_transport_of_dangerous_goods. (Accessed on 10/29/2018).

[14] William C Frank, Jean-Claude Thill, and Rajan Batta. Spatial decision support system for hazardous material truck routing. *Transportation Research Part C: Emerging Technologies*, 8(1-6):337–359, 2000.

[15] Erik Hofmann and Marco Rüsch. Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry*, 89:23–34, 2017.

[16] Seyoung Huh, Sangrae Cho, and Soohyung Kim. Managing iot devices using blockchain platform. In *Advanced Communication Technology (ICACT), 2017 19th International Conference on*, pages 464–467. IEEE, 2017.

[17] Adnan Imeri, Abdelaziz Khadraoui, and Djamel Khadraoui. A conceptual and technical approach for transportation of dangerous goods in compliance with regulatory framework. *Journal of Software*, 12(9):708–722, 2017.

[18] Chun-Feng Liao, Sheng-Wen Bao, Ching-Ju Cheng, and Kung Chen. On design issues and architectural styles for blockchain-driven iot services. In *Consumer Electronics-Taiwan (ICCE-TW),*

2017 IEEE International Conference on, pages 351–352. IEEE, 2017.

[19] Carlo Maria Medaglia and Alexandru Serbanati. An overview of privacy and security issues in the internet of things. In *The Internet of Things*, pages 389–395. Springer, 2010.

[20] Gemma Dolores Molero, Francisco Enrique Santarremigia, Pablo Aragonés-Beltrán, and Juan-Pascual Pastor-Ferrando. Total safety by design: Increased safety and operability of supply chain of inland terminals for containers with dangerous goods. *Safety science*, 100:168–182, 2017.

[21] Taewoo Nam and Theresa A Pardo. Conceptualizing smart city with dimensions of technology, people, and institutions. In *Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times*, pages 282–291. ACM, 2011.

[22] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. Blockchain. *Business & Information Systems Engineering*, 59(3):183–187, 2017.

[23] Ebru Vesile Ocalir-Akunal. Decision support systems in transport planning. *Procedia engineering*, 161:1119–1126, 2016.

[24] Alfonso Panarello, Nachiket Tapas, Giovanni Merlino, Francesco Longo, and Antonio Puliafito. Blockchain and iot integration: A systematic survey. *Sensors*, 18(8):2575, 2018.

[25] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. On blockchain and its integration with iot. challenges and opportunities. *Future Generation Computer Systems*, 2018.

[26] Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, and Nada Chendeb Taher. Towards using blockchain technology for iot data access protection. In *Ubiquitous Wireless Broadband (ICUWB), 2017 IEEE 17th International Conference on*, pages 1–5. IEEE, 2017.

[27] Vincenzo Torretta, Elena Cristina Rada, Marco Schiavon, and Paolo Viotti. Decision support systems for assessing risks involved in transporting hazardous materials: A review. *Safety science*, 92:1–9, 2017.

[28] UNECE. Unece homepage. `https://www.unece.org/info/ece-homepage.html`. (Accessed on 10/29/2018).

[29] N Vayiokas. Risk assessment of transportation of dangerous goods.

[30] Ningkui Wang, Xiaozhong Huang, and Daijun Wei. Route selection for dangerous goods based on d numbers. In *Control and Decision Conference (CCDC), 2016 Chinese*, pages 6651–6656. IEEE, 2016.

[31] Wenbo Wang, Dinh Thai Hoang, Zehui Xiong, Dusit Niyato, Ping Wang, Peizhao Hu, and Yonggang Wen. A survey on consensus mechanisms and mining management in blockchain networks. *arXiv preprint arXiv:1805.02707*, 2018.

[32] Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. A taxonomy of blockchain-based systems for architecture design. In *Software Architecture (ICSA), 2017 IEEE International Conference on*, pages 243–252. IEEE, 2017.

[33] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao. A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal*, 4(5):1250–1258, 2017.

[34] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where is current research on blockchain technology?a systematic review. *PloS one*, 11(10):e0163477, 2016.

[35] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, and Huaimin Wang. Blockchain challenges and opportunities: A survey. *Work Pap.–2016*, 2016.

[36] Konstantinos G Zografos and Konstantinos N Androutsopoulos. A decision support system for integrated hazardous materials routing and emergency response decisions. *Transportation Research Part C: Emerging Technologies*, 16(6):684–703, 2008.

Communication Technologies integration into the Electrical System of the city of Praia

Claudino Mendes[1] and Mateus Andrade[1]

[1]Universidade de CaboVerde, Praia, Cabo Verde.
Claudino.mendes@docente.unicv.edu.cv,
mateus.andrade@docente.unicv.edu.cv

Abstract

The electric sector in small island states, such as Cape Verde, have many related weaknesses, such as: high percentage of commercial losses - mainly theft, difficulty in integrating renewable energy and lack of quality in energy supply, which has reflected in a high cost of electricity. In this sense, Smart Grid technologies have been one of the main bets to guarantee the sustainability of the ES in these regions, to improve its reliability, to maximize its energy efficiency and to increase its robustness. Thus, the integration of technologies such as: SCADA / EMS / DMS, Smart Meters and DER, requires a two-way communication system that interconnects the whole system, allowing to monitor and control the entire electrical network, giving it the ability to identify and correct almost instantly, the constraints caused by demand. This paper presents an architecture proposal for the communication system that could be coupled with the ES of Praia, as a way to guarantee the integration and communication of SG technologies, as well as to enable new applications and services that would assist in the management of all sector. The proposed communication system architecture results from the application of international precepts and norms as well as the results obtained through simulation software, taking into account the existing endogenous technologies and the geographic and socioeconomic conditions of the city.

Keywords: Smart grid, Communication Technologies, Electrical system (ES).

1. Introduction

Investment in smart, modern and robust electricity networks is an undeniable need for small island states because, in most cases, despite their scarce natural resources, have excellent renewable resource use conditions as sun and wind. This requires an electrical management and control system with specific attributes needed to answer the many adversities inherent in their condition, usually associated with high dependence on oil, the difficulty of renewable energy integration, inefficiency and ineffectiveness of electrical networks, and that of course entails large power losses and a high cost of electricity for consumers [1].

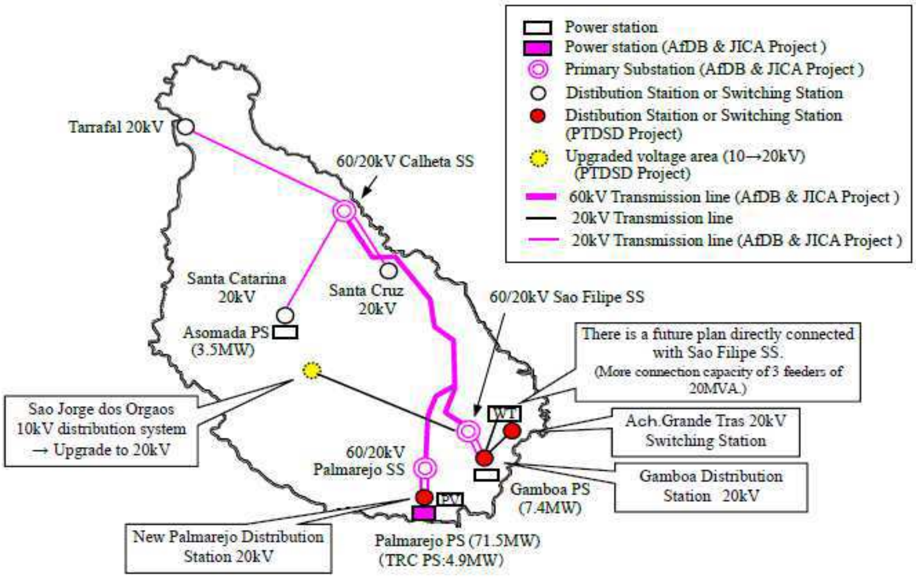
Smart Grid technologies emerge as a natural alternative for those wishing to improve the performance of its energy systems, especially with respect to minimizing technical losses, eliminating energy theft, the integration of distributed renewable energy and reduction of environmental impact , as it allows managing energy storage, improving communication between the various subsectors of the electrical system (ES), managing the integration of renewables and controlling the levels of CO2 emissions in all stages of ES [2]. In this process, communication systems have a key role, both in the process of transmission, analysis and data control, as in the monitoring process and in decision making, working at various levels of the electrical system: the production, through transmission and distribution to the final consumer [3].

This article aims to evaluate the integration of communication systems in a smart grid on an island system and define the requirements and structure of communication systems that best adapted to their ES, considering its geographical feature and the availability of existing infrastructure, taking as case studies the city of Praia, Cape Verde. The study presents a communication architecture proposal for a smart grid taking into account the technical and economic aspects of the grid and existing communication infrastructures as well as the geography of the archipelago.

2. Electrical and Communication System of the city of Praia.

The ES of the city of Praia works integrated way with the ES of the island of Santiago, and the network that is has a high-voltage transmission lines (HV) with a 60kV voltage, which connects the island of the ES, and distribution network Medium voltage (MV) with a 20kV voltage, which feeds the various processing stations of the island. The electrical supply is provided by a diesel power plant, wind farm and photovoltaic power plant, according to figure 1 [4]. The distribution network is the electrical system of the sector with the highest deficit, where the absence of a communication system it is noted more clearly. The way the monitoring and control has been carried out does not allow the concessionaire to fully answers the constant requests in terms of operating and maintaining the network, new customer request, network expansion and integration of microgeneration. However the issue of loss remains the most worrying whether technical losses or commercial losses, including theft and burglary. In 2016 the values of electrical losses were more than 1/3 of the production.

On the other hand, in terms of communication system, the widespread use of wireless technologies has allowed to the city give answers timely and appropriate the constant demands of the demand of the ICT sector, both in terms of quality of service availability, as the level of introduction these technologies in the various state sectors, including as a tool to assist in governance. According to the report of the National Communications Agency (ANAC) for the second quarter of 2016, the penetration rate of mobile devices was 118% in relation to population, internet services had a total of 312,940 signatures, mainly through 3G technology, introduced in 2011 and accounted for 261,693 subscribers, corresponding to 56% of the population and the ADSL internet service with a 2.8% penetration rate [5].


Power station
Power station (AfDB & JICA Project)
Primary Substation (AfDB & JICA Project)
Distibution Staition or Switching Station
Distibution Staition or Switching Station (PTDSD Project)
Upgraded voltage area (10→20kV) (PTDSD Project)
60kV Transmission line (AfDB & JICA Project)
20kV Transmission line
20kV Transmission line (AfDB & JICA Project)
Tarrafal 20kV
60/20kV Calheta SS
Santa Catarina 20kV
Santa Cruz 20kV
60/20kV Sao Filipe SS
Asomada PS (3.5MW)
There is a future plan directly connected with Sao Filipe SS. (More connection capacity of 3 feeders of 20MVA.)
Sao Jorge dos Orgaos 10kV distribution system → Upgrade to 20kV
WT
Ach.Grande Tras 20kV Switching Station
60/20kV Palmarejo SS
Gamboa Distribution Station 20kV
Gamboa PS (7.4MW)
PV
New Palmarejo Distribution Station 20kV
Palmarejo PS (71.5MW) (TRC PS:4.9MW)

Source: JICA Study Team

Figure 1 - Layout of Santiago's electric transmission network.

The most commonly used wireless technologies are: GSM, 3G and WiMAX, its characteristics are shown in table 1. The 3G network uses radio frequency (RF) technology and provide the data and voice services. The WiMAX system is based on the IEEE 802.16-2005 standards and the WiMAX Forum, it also provides data, voice and video services used exclusively by private state network [6]. ADSL is the most widely used technology wired then the optical fiber has increased its use every year. This technology uses copper cable to provide data and voice services covering all parts of the city, the GSM technology is used for communication services with a high rate of coverage.

Technology	Spectrum	transmission rate	Coverage	Application on
GSM	890 – 935 MHz	< 14.4 Kpbs	1 -10 Km	Mobile Communication
GPRS	1800-2100 MHz	< 170kbps	1 -10 Km	Mobile Communication
3G	2.11-2.17GHz	2Mbps	1 -10 Km	Data, Voice, Video
WiMAX	2.56-2.63 GHz	< 25Mbps	10-50Km (LOS) 1-5Km (NLOS)	Data, Voice, Video

Table 1 - Features of wireless technologies in the city of Praia.

3. Communication systems for Smart Grid

Smart grid is a technology that allows the ES interconnection and interaction between all the elements associated with it through advanced communication technologies, monitoring and control, in order to efficiently provide electricity for economic, safe and sustainable manner, benefiting producers, distributors and consumers [7]. The operation of the SG is leveraged in a number of technologies and applications, connected to sensors and actuators through a bidirectional communication system connects the entire system, from production through distribution to end users, allowing the dealership to monitor and control all network, giving it the ability to "self-healing", ie ability to identify and correct almost instantaneously the constant constraints caused by demand on the network [8]**.**

3.1. Smart Grid Technologies

As a way to improve the reliability and efficiency of electricity supply, Smart Grid offers a range of technologies whose impact is reflected in the reduction of generation costs and electricity supply to consumers, as follows:

Smart meter and Advanced Metering Infrastructure

Smart Meter (SM) is often referred as an essential requirement in the implementation process of a smart grid, one times, coupled to a bidirectional communication system and a data management center provides enumeras advantage in terms of measurement and counting in all subsectors of the ES [9]. A *Advanced Metering Infrastructure* (AMI) emerges as a technology that involves not only the SM but also an infrastructure that encompasses communications, applications and interfaces, enabling data exchange between the central production and distribution network counters and consumers, figure 2.

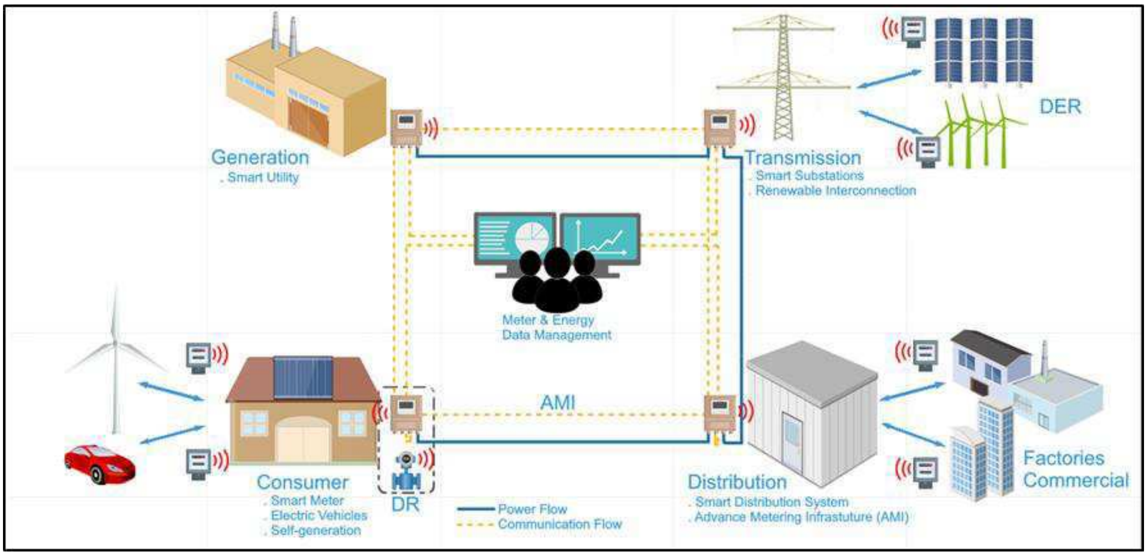


Figure 2 - AMI operating architecture

Energy Management System and Demand Management System

The Energy Management System technology (EMS) is responsible for the management of production systems and substations, this technology covers both production of conventional power plants and renewable production of wind or photovoltaic plants. The EMS technology, based on communication and the various control and measuring device technologies, enables monitor, control and optimize system performance in terms of generation and electricity transmission [10]. The Demand Management System technology (DMS) offers a great deal through the communication system, methods of regulation and economic incentives that can provide as well as other features that enables to optimize the network through a more efficient control of resources and demand by the system operator as well as the reduction of system losses and decreased CAIDI and SAIDI [47].

Distributed energy resources

Through its ability to automatic voltage regulation can control electrical systems with high DER penetration rate, since the problems related to the integration of renewable in the network such as distortion harmonics, voltage variation and synchronization between production and the network can be mitigated based on forecasts and permission of Demand Side Management. These technologies enable distributed generation is injected both in network transmission and in distribution, in addition to storage, allowing it to provide greater reliability and robustness, since the *backup* is always available [11] [12].

3.2. Communication requirements for Smart Grid

For the proper functioning and performance of a SG, it is necessary to define a communications structure that ensures reliability, sophistication and speed and to allow the interconnection and exchange of information between the various network components, such as generators, substations the transformer stations, the storage systems and consumers, either in real time and that benefits all system stakeholders [13]**.** Smart Grid communications are standardized protocols based on allowing the interconnection with the main control unit through a secure communication network structure composed of these three hierarchical layers: *Local Area Network* (LAN), *Home Area Network* (HAN) e *Wide-Area Network* (WAN) [14]. For each of these networks there are several technologies that support them as application, range, or transmission capacity that is intended. The technologies can be wired or wireless, and the most widely used wireless technologies are: 3G, WiMAX, ZigBee or Wi-Fi. These technologies have the advantage of operating with cheaper infrastructure and allow connections in hard to reach areas, but are more vulnerable to external interference in transmission. On the other hand, wired technologies like fiber optics, PLC, Digital Subscriber Line (DSL) and Coaxial Cable, have no interference problems and do not need external power sources such as battery to operate, but the cost of their implementation is higher [15] [16]. This time, the big challenge for electric power companies will be in the definition of reporting requirements and meet in the best communications infrastructure choice and which best fits the reality in which it is framed, in order to ensure a safe, affordable and reliable.

4. Architecture grid based on communication and information technologies

The new layout propose a communication structure that ensures a two-way communication to and from all levels of the electronic system communication based on an array of sensors, actuators, accelerometer and Phasor Measurement Units (PMU) to be integrated network, enabling him to make available to the operations and monitoring center all information related to the operation of the electrical network Figure 33.

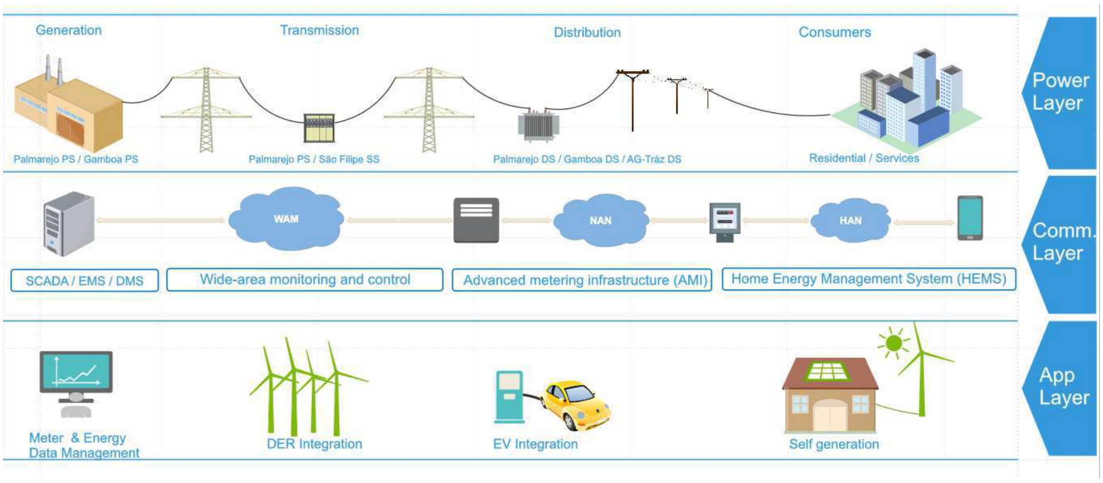

Generation
Transmission
Distribution
Consumers
Power Layer
Palmarejo PS / Gamboa PS
Palmarejo PS / São Filipe SS
Palmarejo DS / Gamboa DS / AG-Tráz DS
Residential / Services
WAM
NAN
HAN
Comm. Layer
SCADA / EMS / DMS
Wide-area monitoring and control
Advanced metering infrastructure (AMI)
Home Energy Management System (HEMS)
App Layer
Meter & Energy Data Management
DER Integration
EV Integration
Self generation

Figure 3 - Smart Grid system layout to the city of Praia.

The proposed WAN network covers a wide geographic area encompassing the LANs of the exchanges and the substation networks, also known as the backhaul network. This network would enhance the existing dispatch system SCADA / EMS / DMS, mainly in the ER production management integration in the electricity grid. The proposed communication technology to support the network would be a hybrid system using fiber optic and telecommunication operators 3G technology for the transmission of data between production centers and substations [17]. On the other hand to ensure communication in the distribution network from substation distribution to consumers, it proposes the creation of several neighborhood area networks (NAN) or Field Area Network (FAN) based on GSM and GPRS communication technology, or 3G technology. This proposal was based on simulation results with Atoll software as figure 4. Each network NAN result of the aggregation of several SM within a neighborhood around an aggregator / data collector to form a neighborhood network. In turn each data collector would connect to the backhaul network of the WAN, enabling full communication from the SM and other control device, consumers through the automatic counting system in Transformation Station, to the central server located in the center of control of power plants [17] [18].

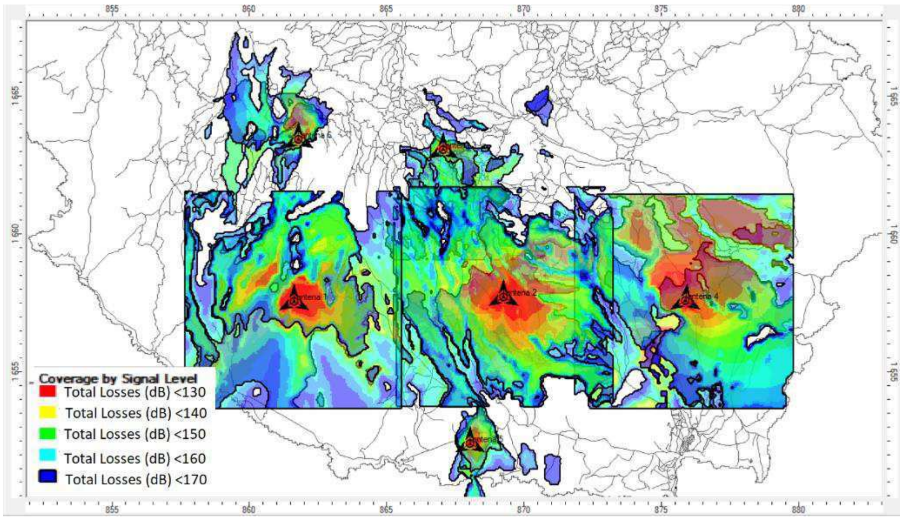


Figure 4 - Import map GSM from Atoll software.

This communication structure would provide the entire electrical system intelligence helping him to monitor, manage, measure and intervene in real time in all sectors, from production to final consumers via EMS and AMI with the possibility of DR, with the ADSL and 3G communication technologies, due to their transmission capacities and levels of territorial coverage. At the consumer level, several HAN, BAN and IAN networks are proposed for residential, commercial and industrial consumers respectively. These networks would allow the interconnection of the SM with the intelligent devices of residences or buildings, residential automation systems, energy storage systems, microgeneration and electric vehicles, separately or together [19]. The HAN network ensure communication between the accounting systems of each individual consumer and the utility, through technologies such as ZigBee, WiFi, ZWave, GSM or Ethernet [14] [20].

5. Conclusion and recommendations

In the city of Praia are being tested some pilot projects such as: SCADA / EMS / DMS, smart meters and DER integration. However, what is observed is that these projects have been tested in an individualized and disintegrated way, so that the results are not at the desired level, in this sense one of the essential components for this effective integration would be the telecommunication infrastructures. The architecture proposed here aimed to define the requirements and structure of the communication systems that best would adapt to the ES taking into account its geographical characteristics and the availability of existing infrastructures. It became clear that at this stage, due to the mentioned ES characteristics, a hybrid communication structure combining fiber optics with GSM and 3G would be the one that would best meet the requirements. These infrastructure when integrated with ES, improve system reliability; increase the physical security of its components; facilitate the operations, maintenance and repair; facilitate communication with consumers, improve the process of measuring and billing of energy use; increase energy efficiency; enable a better integration of renewable energies as well as electric vehicles, and reduce peak demand with consequent economic and environmental gains. It is recommended for the effective implementation of the Smart Grid in the city, which enhance cooperation, coordination and communication among the various industry stakeholders, the need to improve or create regulations for this purpose, which approves new policy guidelines for planning and management of the ES, directed to Smart Grid

References

[1] Scheneider Electric, "Island Micro-grid," in *Cabo Verde Micro-grid*, Praia, 2014.

[2] M. E. El-hawary, "The Smart Grid State-of-the-art and Future Trends," in *Electric Power Components and Systems*, vol. 42, T. &. F. Group, Ed., Taylor & Francis Group, 2014, p. 3–4.

[3] V. C. Gungor, "Smart Grid Technologies: Communication Technologies and Standards," *IEEE Transactions on Industrial Informatics,* vol. 7, p. 530, 2011.

[4] Japan International Cooperation Agency, "The Study of Information Collection and Verification Survey for Renewable Energy Introduction and Grid Stabilization in the Republic of Cabo Verde," Praia, 2016.

[5] Agencia Nacional das Comunicações - ANAC, "Indicadores Estatísticos do Mercado das Comunicações Electrónicas em Cabo Verde - Segundo Trimestre 2016," 2017. [Online]. Available: http://anac.cv/index.php?option=com_content&view=article&id=504%3Aindicadores-estatisticos-segundo-trimestre-2016&catid=34%3Aanuncios&Itemid=63&lang=en. [Accessed 7 Janeiro 2017].

[6] Nucleo operacional para a sociedade de informação (NOSi), *Projecto de Upgrade da Plataforma de Governação Electrónica,* Praia, 2009.

[7] Global Smart Grid Federation, "Smart Grid," Global Smart Grid Federation, 2017. [Online]. Available: http://www.globalsmartgridfederation.org/smart-grids/. [Accessed 15 Fevereiro 2017].

[8] M. a. A. J. A. G. N.Zareen, "Worldwide Technological Revolutions and Its Challenges under Smart Grid Paradigm: A Comprehensive Study," *International Journal of Scientific & Engineering Research,* vol. 3, no. 11, pp. 1- 6, 2012.

[9] I. C. R. Bayindir, "Smart grid technologies and applications," *Renewable and Sustainable Energy Reviews,* vol. 66, p. 499–516, 2016.

[10] C. P. A. D. Prabhash Nanda, "Energy Management System in Smart Grid: An Overview," *International Journal of Research and Scientific Innovation,* vol. II, no. 12, pp. 31-38, 2015.

[11] A. Mahmood, "A review of wireless communications for smart grid," *Renewable and Sustainable Energy Reviews ,* vol. 15, pp. 248-260, 2015.

[12] M. K. T. M. K.S. Reddy, "A review of Integration, Control, Communication and Metering (ICCM) of renewable energy based smartgrid," *Renewable and Sustainable Energy Reviews,* vol. 38, p. 180–192, 2014.

[13] V. C. Gungor, "A Survey on Smart Grid Potential Applications and Communication Requirements," *IEEE transactions on industrial informaticS,* vol. 9, pp. 28-41, 2013.

[14] M. Kuzlu, M. Pipattanasomporn and S. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN," *Computer Networks,* vol. 67, pp. 74-88, 2014.

[15] International Energy Agency (IEA) , "www.iea.org," 2011. [Online]. Available: https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf. [Accessed 15 Fevereiro 2017].

[16] M. P. M. Kuzlu, "Assessment of communication technologies and network requirements for different smart grid applications," in *IEEE Innovative Smart Grid Technologies (ISGT) Conference*, 2013.

[17] Qualcomm, "3G Cellular Technology for Smart Grid Communications," 2012. [Online]. Available: https://www.qualcomm.com/documents/3g-cellular-technology-smart-grid-communications. [Accessed 04 11 2016].

[18] F. Bouhafs, M. Mackay and M. Merabti, "The Smart Grid in the Last Mile," in *Communication Challenges and Solutions in the Smart Grid*, SpringerBriefs in Computer Science, 2014, pp. 25-35.

[19] R. R. Mohassel, A. S. Fung, F. Mohammadi and K. Raahemifar, "A Survey on Advanced Metering Infrastructure and its Application in Smart Grids," in *IEEE 27th Canadian Conference* , Toronto, ON, Canada, 2014.

[20] S. Borlase, "Communications Systems," in *Smart Grids: Infrastructure, Technology, and Solutions*, Taylor & Francis Group, 2013, pp. 266-294.

Security Issues In Hybrid Approaches: Context-Based And Software-Defined Networks

Robson Gonzaga Silva[1] and Paulo N. M. Sampaio-PhD[2]
Salvador University - UNIFACS, Salvador, Brazil.
Professor.robsongonzaga@gmail.com, pnms.funchal@gmail.com

Abstract

Abstract — **The application of experimental networks through the proposal of hybrid networks such as the combination of Context-based and Software Defined Networks (SDNs) is a promising approach due the combination of their main benefits such as scalability, dynamism, flexibility, easy management and function control, programming, etc. Nevertheless, depite the advantages of these hybrid approaches, the study of the literature unveals some existing security challenges and drawbacks in these approaches. This paper aims at identifying and discussing the existing vulnerabilities and security issues in hybrid models such as CAARF-SDN, presenting through some illustrative scenarios how these attacks can take place and proposing some possible solutions in order to prevent these attacks.**

Keywords‒ SDN, Context-Based Networks, Security Issues, CAARF-SDN.

Introduction

The demand for an optimized management of the available resources of the network infrastructure is growing exponentially in order to cope with the co-existence of the also growing heterogeneous traffic in the Internet. Therefore, since Internet was not designed to meet this demand, issues such as vulnerability, instability, scalability and incompatibilities are more evident as well. The success and growth of Internet is undeniable, however some of its limitations are being unveiled, thus it is important to reconsider its architecture and main protocols with new experimental networks.

In order to improve user□s experience and embody the concept of a user-centered network the notion of context can be applied. Context awareness is understood as an ubiquous and pervasive computing paradigm where the computational environment reacts according to the changes in its current state (Shaikh & Fiedler, 2010). The implementation of context aware networks can be helpful in order to improve user□s satisfaction when accessing network resources and to enrich traffic management since it considers users, network and end-user devices requirements, providing a generic and cutting-edge approach for traffic optimization.

In this context, another important paradigm are the Software Defined Networks (SDN) which provide the required mechanisms for the implementation of a dynamic control architecture and management of network resources in order to deliver heterogeneous traffic due to the decoupling of control plan and routing plan (Kim & Feamster, 2013). Nevertheless, flowtable configuration within SDNs controllers is still carried out statically, which does not allow the description of the dynamic nature of context-based networks.

In order to provide the dynamic configuration of SDN networks, in this work we propose the application of a user-centric (context-based) optimization solution to SDNs called *Context-Aware Adaptive Routing Framework* - applied to SDN networks (also called CAARF-SDN) (Muakad, 2015)

(Oliveira, 2015) (Silva, 2015) (Spinola, 2015). Hybrid networks such as CAARF-SDN rely on the integration of the concepts of Quality of Service (QoS), Quality of Experience (QoE) and Quality of Device (QoD) in order to provide a more proactive and dynamic approach for time-sensitive traffic delivery (such as VoIP and video), while aiming at the improvement of user perception over a conventional and experimental IP networks.

By the combination of Context-based and Software Defined Networks (SDNs) in a hybrid model it is possible to sum the benefits of both paradigms, such as scalability, dynamism, flexibility, easy management and function control, programming, etc. (Young et al., 2017) (Porras et al., 2012) (Shin et al., 2014). Meanwhile, some challenges and drawbacks can also be minimized with this hybrid approach, in particular, the static management of SDN configuration tables. The automatic configuration of SDN switches has already been addressed in the literature (Spinola, 2015) (Bentaleb et al., 2017) (Dobrijevic et al., 2014) (Owens & Durresi, 2014) in MPLS based hybridization in SDN, however none of the approaches provide dynamic configuration of flow tables.

Nevertheless, despite the several advantages of these hybrid approaches, the CAARF-SDN paradigm also introduces new vulnerabilities and threats. According to (Porras et al., 2014) SDNs, in particular, present new challenges for security in computer networks affecting authenticity, integrity and availability. Therefore, this paper aims at identifying and discussing the existing vulnerabilities and security issues in hybrid models such as CAARF-SDN and finally propose some possible solutions for these limitations.

This paper is organized as follows: Section II presents and discusses some network optimization related works identified in the literature; Section III introduces context-sensitive systems and presents the adopted context model; Section IV presents the CAARF-SDN architecture; Section V discusses a case study and section VI presents the conclusions of this paper and some perspectives for future work.

Context-Aware Adaptative Routing Framework (CAARF-SDN)

The Context-Aware Adaptive Routing Framework applied to SDN Networks (also called CAARF-SDN) (Muakad, 2015) (Oliveira, 2015) (Silva, 2015) (Spinola, 2015) is a conceptual context-based solution proposed for traffic optimization within SDN networks. The conceptual architecture of CAARF-SDN is illustrated in Figure 1 and it is composed of the following modules: Context Reader, Optimization and Flowtable Configuration.

The ***Context Reader*** module aims at collecting the QoS, QoD and QoE notifications from their respective sources (network devices, end-user devices and users) and process them in order to verify the global context of the system (QoC). These data are used by the other modules of CAARF-SDN in order to support traffic optimization decisions. If a relevant context modification is verified a notification for the optimization module is issued.

The ***Optimization Module*** aims at automatically selecting the existent optimal paths based on contextual information generated by the *Context Reader Module*. The path selection relies on a set of pre-defined policies, built upon data analysis and performance indexes also generated by the *Context Reader Module*. Therefore, when a context variation notification is generated by the *Context Reader Module*, the *Optimization Module* analyzes the network topology dynamically, determining the optimal forwarding paths. This analysis relies on a ranking approach applied to the existing paths using their respective QoC metrics. At last, the *optimization module* sends to the *Flowtable Configuration* module the configuration directives that have to be applied on the SDN controller□s flowtable.

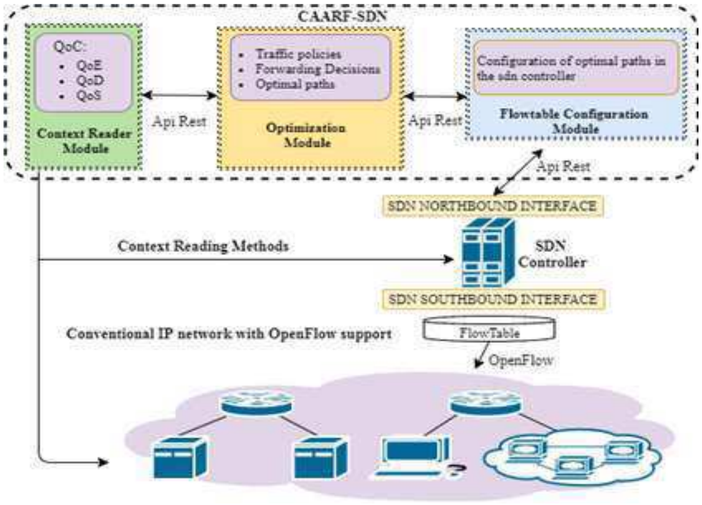


Figure 1: CAARF-SDN Conceptual Architecture

The main goal of the ***Flowtable Configuration*** module is to set the SDN controller’s flowtable dinamically based on the configuration directives issued by the *optimization module*. This configuration is carried out through the SDN controller API functions, using the controller’s Northbound interface. Once the controller’s flowtable is reconfigured, it updates the SDN switches’flowtable using its *Southbound* interface.

Cases Scenarios: Exploring Vulnerabilities Within CAARF-SDN

In order to implement the CAARF-SDN architecture it is important to take into account the security issues and mitigate the potential vulnerabilities in this solution. Since CAARF-SDN is a context-based approach which relies on a Software-Defined Network, most of its vulnerabilities and threats within this new model are inherited from the SDN architecture. Therefore, in the previous section some of the SDN’s main vulnerabilities and threats are discussed and, further on, we also discuss some of the proposed solutions.

a. MAN IN THE MIDDLE Attack

This scenario illustrates the *Man-in-the-Middle* attack which affects integrity within CAARF-SDN in different ways: (i) the context notification messages collected by the CAARF-SND’s *Context Reader Module* can be modified; (ii) the configuration directives sent by the *Flowtable Configuration Module* can also be intercepted and modified before configuring the controller’s flow table; (iii) the flow rules configured within SDN controller’s flow table can be modified, and; (iv) the OpenFlow messages can be forged when accessed by the switches (Kevin Benton et al.; Sandra Scott et al.; ONF). These attacks within the CAARF-SDN architecture are illustrated in Figure 2.

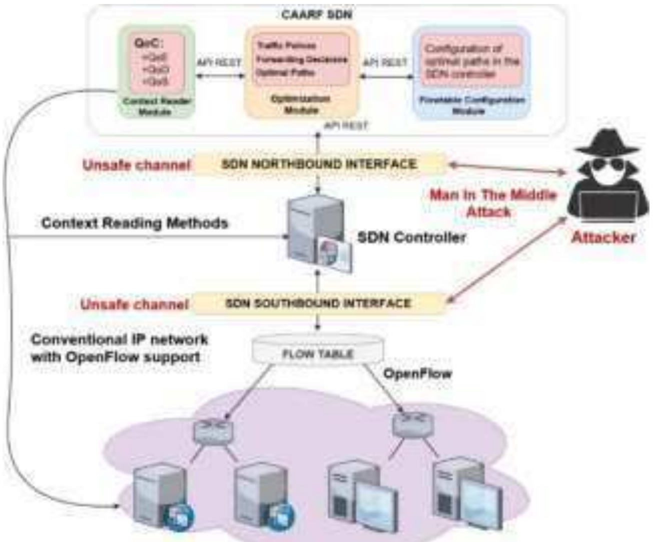


Figure 2: Illustration of a *Man In The Middle* attack within CAARF-SDN.

Figure 2 illustrates these attacks and, in a first attempt, the attacker is able to intercept and modify the context notifications sent to CAARF-SDN. Therefore, with forged context messages the CAARF-SDN mechanisms will not be able to correctly optimize the traffic delivery.

Furthermore, the attacker would also be able to explore the interface between *Application Layer* and *Control Layer*, capturing the configuration directives sent from CAARF-SND to the SDN Controller through a vulnerable communication channel of the Controller□s Northbound interface. Through this attack the controller□s configuration directives can be inserted, the existing ones modified or excluded, affecting the correct behavior of the SDN devices (Young et al. 2017) (Migault, 2016) (ONF, 2013). Furthermore, the behavior of the SDN devices can also be affected if the attacker is able to access and reconfigure the controller□s flowtable, forging false and incorrect switching rules.

At last, another vulnerability is also present in the communication channel between the *Control Layer* and the *Data Layer* determined by the controller□s Southbound interface. This attack would also affect the integrity of the flowtable content leading to the incorrect configuration of the SDN devices.

The lack of solutions related to cryptography and traffic control mechanisms are related to these vulnerabilities within Context-based SDN networks (Migault, 2016) (Porras et al., 2015).

Some strategies and measures are proposed in the literature in order to increase the security level against this type of attack (Shun et al., 2016) (Nigan et al., 2016) . For instance, the implementation of cryptography mechanisms within SDN networks is broadly discussed in the literature since due the lack (and complexity) of implementation of TLS/SSH on communication channels (Northbound and Southbound) between the *Application* and *Control layers* data remain vulnerable (Young et al. 2017) (Shu et al., 2016). Nevertheless, since the main goal of CAARF-SDN is the network traffic optimization, performance issues should not be neglected. Therefore, considering that the implementation of cryptography would bring an extra latency to CAARF-SDN processing, this solution is not applicable in this scenario.

In contrast, as for the deployment of traffic control mechanisms, they are useful to implement rules for monitoring, inspection and permission control of traffic within the network. For this purpose, the utilization of tools such as *FortNox* (Porras et al., 2017), *VeriFlow* (Zhou et al., 2012) and *Flowchecker* (Young et al. 2017) are commonly referred in the literature (Hayward, 2012) (Shu et al., 2016). Therefore, the traffic control can be a potential solution to man in the middle attack within CAARF-SDN without affecting performance.

b. DDoS Attack

This scenario is related to an attack that affects the availability of resources called (Distributed) *Denial of Services* (DDoS). In this case, this attack would affect directly either (or both) the CAARF-SDN architecture and the SND controller (Shu et al., 2016) (Porras et al., 2015) (Cheung et al., 2015). This scenario is depicted in Figure 3.

In this scenario illustrates how an attacker can make several Application Layer devices (also called Zombie PCs) to proceed with a number of requirements (of the *Packet In* type) to the controller through packet flooding, overloading the controller and consequently leading to its unavailability. It is important to note that the same attack can be carried out towards the CAARF-SDN service as well.

These type of attacks can take place either locally or remotely taking advantage of some vulnerabilities such as the lack of traffic control in the communication channels (northbound and southbound), weak authentication mechanisms and inappropriate configuration of network devices (Yoon et al., 2017) (Shu et al., 2016) (ONF, 2013) (Nigam et al., 2016).

As it is well known, DDoS attacks are hard to detect when one service is under attack. However, preventive measures can be adopted in order to mitigate (or at least reduce) this type of attack. In order to prevent these DDoS attacks, two main solutions are proposed in the literature: the implementation of traffic control and redundancy.

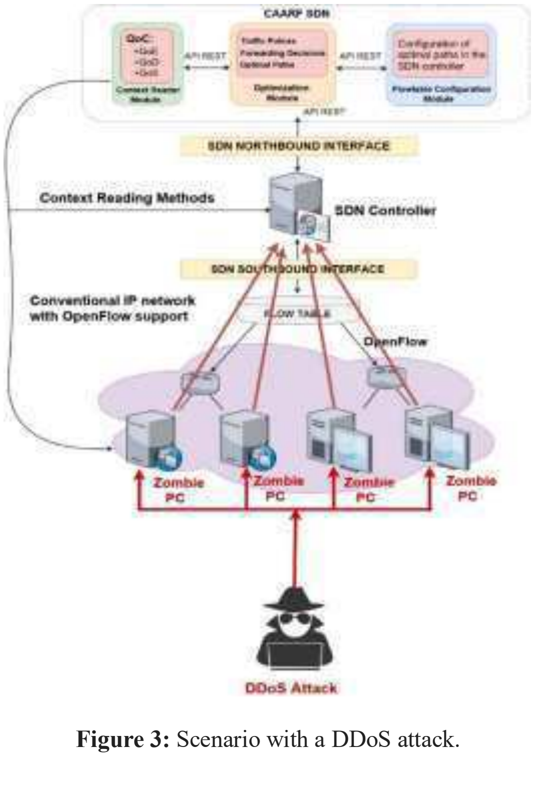


Figure 3: Scenario with a DDoS attack.

With the implementation of traffic control it is possible to identify and filter traffic according to its origin, destination, service, etc., and also according to the OpenFlow rules defined to a particular traffic. In this case, the good practices introduced in the literature are to limit the transmission rate within OpenFlow communication channels among *Application*, *Control* and *Data layers* aiming at preventing flooding traffic with requirements (In Packet) to the OpenFlow Controller, and avoidind it to become unavailable. The tools applied in general for the implementation of traffic control are *FortNox*, *VeriFlow*, *FlowChecker*, among others.

Another security strategy applied to prevent DDoS attacks is the implementation of redundancy of the main services in the platform, such as the SDN Controller and the CAARF-SDN platform. For instance, a possible solution introduced in (Shu et al., 2016) presents the deployment of three collaborative SDN Controllers physically distributed but logically centralized, exchanging information about the general perspective of the network through two new interfaces (*Eastbound* and *Westbound*). In this approach, it is important the compatibility of the SDN Controller with mirroring and collaborative features. Currently, the SDN Controllers such as FloodLight Cheung et al., 2015), OpenDayLight and Nox (Rothenberg & Nascimento, 2011) are compatible with these features (Yoon et al., 2017). It is interesting to (Zimmermann, 2007) note that this approach can be similarly applied to the *Application Layer* by the implementation of redundancy of the CAARF-SDN services. In this case, physical decentralization of these services would foster scalability, availability and effectiveness of CAARF-SDN□s services.

c. Malicious *Software (M*alwares) Attack

This scenario illustrates the attack carried out by malicious software (Malware). Malicious software can attack the integrity of CAARF-SDN context information, leading to incorrect context definition and consequently the generation of incorrect optimization configuration (Shu et al., 2016) (ONF, 2013) (Cheung et al., 2015). Figure 4 illustrates this attack.

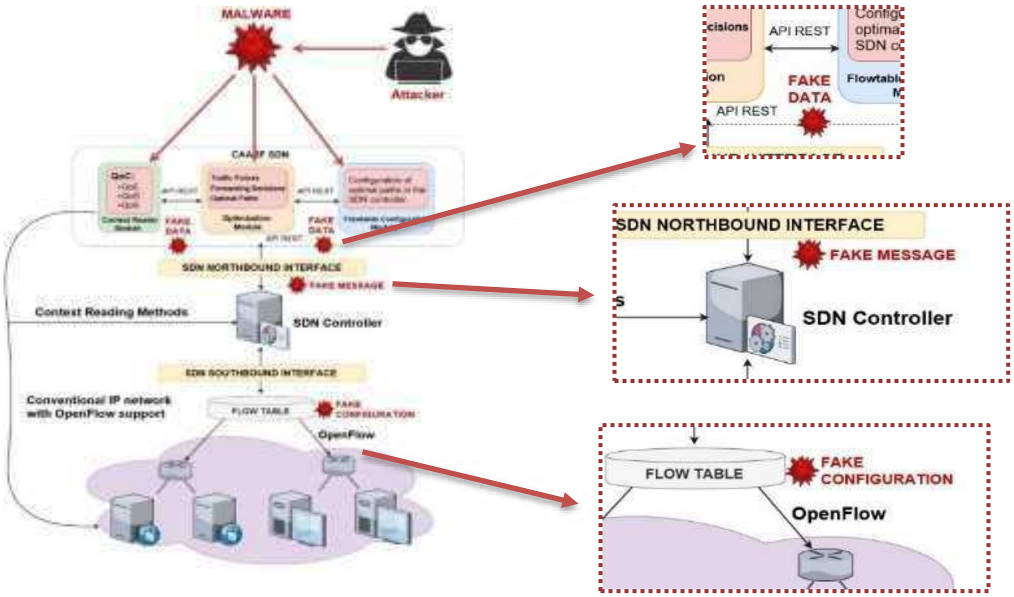


Figure 4: Attack using malware within CAARF-SDN.

Within this scenario, another important target would be the SDN controller itself, which can be infected granting the attacker with the control of the SND network (Shu et al., 2016) (ONF, 2013) (Porras et al., 2015). These kinds of attacks affect the confidentiality and integrity within the network since all the context information can be accessed and forged by the attacker. The lack of authentication and cryptography mechanisms allow attackers to explore these vulnerabilities (Migault,2016) (Röpke & Holz, 2015) (Shu et al., 2016) (Porras et al., 2015).

The utilization of tools such as SEFloodlight, FRESCO and PermOF (Yoon et al., 2017) (Porras et al., 2012) (Shin et al., 2014) (Shu et al., 2016) (Benton et al., 2013) is also proposed in the literature as mechanisms to prevent from malware attacks against SDN networks (Yoon et al., 2017) (Hayward, 2016). This is possible through the authentication of applications which can be identified as reliable or not and through the evaluation of their access control in order to allow them to modify or not the SDN□s Flow Table within the SDN Switch and limit the utilization of the Controller□s resources. This approach prevents that malwares are applied to modify SND rules specified by the network manager (and optimized by CAAR-SDN), as well as imposing a restriction level at the Application layer, ensuring security aspects such as integrity, authenticity, confidentiality and network availability.

Conclusions And Future Works

The analysis of several contributions found in the literature concerning the security aspects within SND networks allowed the identification of common vulnerabilities and potential attacks in these networks, and further clusterization of the main solutions proposed to these attacks. This study allowed us to propose a comparative perspective to hybrid networks such as context-based SDN networks with the application of CAARF-SDN.

Based on the study carried out it was possible to present some illustrative scenarios with these vulnerabilities and attacks, coming up with some potential solutions to these attacks. As for future works, these scenarios and their respective security solutions should be implemented, and a security framework should be proposed to CAARF-SDN.

References

A. L. C. d. Oliveira, “Context-based Notification Mechanism for Adaptive Forwarding,” in *UNIFACS Universidade Salvador*, Salvador, Brasil, 2015.

A. Khurshid, W. Zhou, M. Caesar, and P. B. Godfrey, “Veriflow,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 4, p. 467, 2012.

C.F.J. Muakad, “Context-based Dynamic and Adaptive Forwarding Management,” *UNIFACS Universidade Salvador*, Salvador, Brasil, 2015.

C. Yoon, S. Lee, H. Kang, T. Park, S. Shin, V. Yegneswaran, P. Porras, and G. Gu, “Flow Wars: Systemizing the Attack Surface and Defenses in Software-Defined Networks,” *IEEE/ACM Trans. Netw.*, vol. 25, no. 6, pp. 3514–3530, 2017.

C. Röpke and T. Holz, “SDN rootkits: Subverting network operating systems of software-defined networks,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9384, pp. 337–356, 2015.

D. Migault, “Identifying and addressing the vulnerabilities and security issues of SDN,” no. January 2016, 2015.

J. H. G. Corrêa, V. Nigam, M. Ribeiro, D. Mafioletti, and I. E. Fonseca, “SHADE: Uma estratégia seletiva para mitigar ataques DDoS na camada de aplica ao em redes definidas por software,” pp. 964–969.

J. P. S. d. Silva, “Implementation of an Architecture for the Context-Aware Adaptative Routing Framework (CAARF),” UNIFACS Un., Salvador, Brasil, 2015.

J. Shaikh, M. Fiedler, and D. Collange, “Quality of experience from user and network perspectives,” *Ann. des Telecommun. Telecommun.*, vol. 65, no. 1–2, pp. 47–57, 2010.

H. Kim and N. Feamster, “Improving network management with software defined networking,” *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 114–119, 2013.

M. O. Dobrijevic, A. J. Kassler, L. Skorin-Kapov and Matijasevic, “‘Q-point: Qoe-driven path optimization model for multimedia services,'" 2014, pp. 134–147.

Porras, S. Cheung, M. Fong, K. Skinner, "'Securing the Software-Defined Network Control Layer,'" 2015.

P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, "A security enforcement kernel for OpenFlow networks," *Proc. first Work. Hot Top. Softw. Defin. networks - HotSDN '12*, p. 121, 2012.

P. Porras, S. Cheung, M. Fong, K. Skinner, and V. Yegneswaran, "Securing the Software-Defined Network Control Layer," *Ndss '15*, no. February, pp. 8–11, 2015.

R. J. H. Owens, A. Durresi, "'RVSDN: Reliable video over softwaredefined networking,'" in *in: 2014 IEEE Global Communications Conference*, 2014, pp. 1974– 1979.

R. Z. and S. H. A. Bentaleb, A. Begen, "Zimmermann and S. Harous, 'SDNHAS: An SDN-Enabled Architecture to Optimize QoE in HTTP Adaptive Streaming,'" *IEEE Trans. Multimed.*, pp. 1–1, 2017, 2017.

S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," *SDN4FNS 2013 - 2013 Work. Softw. Defin. Networks Futur. Networks Serv.*, pp. 1–7, 2013.

S. Shin, Y. Song, T. Lee, S. Lee, J. Chung, P. Porras, V. Yegneswaran, J. Noh, and B. Byunghoon Kang, "Rosemary: A Robust, Secure, and High-Performance Network Operating System," 2014.

S. S. Spinola, "Context Management applied to Adaptive Forwarding within Convergent Solutions," *UNIFACS Univ. Salvador*, 2015.

Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, "Security in Software-Defined Networking: Threats and Countermeasures," *Mob. Networks Appl.*, vol. 21, no. 5, pp. 764–776, 2016.

A Testbed Tool for Comparing Usability and Security of Mobile Authentication Mechanisms

KarimaBoudaoud[1], Marco Winckler[1], Zauwali S. Paki[1], Philippe Palanque[2]
[1]Université Côte d'Azur, CNRS, I3S, France
[boudaoud, winckler]@univ-cotedazur.fr,
zauwali.sabitu.paki@gmail.com
[1]Université Paul Sabatier, IRIT, France
palanque@irit.fr

Abstract

In this paper, we are concerned by the configuration of authentication mechanisms and how tuning parameters values might affect at the same time the usability and the security of systems. Both usability and security are important properties for interactive systems however, tuning the application (for example to reduce the number of trials) to favor one property (such as security) might decrease another (usability), and vice-versa. In order to investigate the dependencies between usability and security, we propose in this paper a testbed environment for supporting the comparative assessment of authentication mechanisms. The tool presented in this paper allows varying parameters of authentication mechanisms to settle multiple configurations. It integrates a log mechanism for precisely recording the users' interactions. The current implementation features a mobile application that embeds three authentications mechanism, namely: PIN code, Android Pattern Lock and Passface. Nonetheless, the approach can be easily extended to include other authentication mechanisms. The ultimate goal of this testbed is to support user testing of authentication mechanisms and compare the relationship between user's behavior and risk assessment of multiple configurations.

1 Introduction

In contemporary world, the most valuable resource is no longer oil but data and this is one of the reasons why we should care for personal data protection. Currently, lots of personal data (and password granting access to personal data elsewhere) are readily available from personal devices. Mobile devices become so powerful in the last years that they are slowly replacing desktop computers in many users' daily tasks including accessing online services such as managing banking accounts, browsing the Web, managing personal information and professional data including personal contacts and agenda, editing and transporting professional documents. The need of securing mobile devices is thus obvious. Among the threats, unauthorized access to data is the most common and for that many user authentication mechanisms have been proposed in the last years [2].

It is interesting to notice that authentication mechanisms are a user-dependent issue, for that we have to take users capabilities and skills into account when assessing the technology. Jonathan Grudin [3] found that users would subvert any technology that did not directly benefit them in a group-based technological environment. As highlighted by Renaud [4], this finding appears to apply to authentication mechanisms too: people often work around these mechanisms, which are put there explicitly to protect them, because they do not fully understand the benefits that will accrue from observation of security guidelines. For example, too complex polices (e.g., long sequences of characters, numbers and special codes) are harder to remember so many users are tempted to make use of remembering aids (including post it visible over the computer). In other words, the efficiency of authentication mechanisms also depends on the overall usability of the interactive system and the security policies that implement it.

The usability is defined by the standard ISO 9241-11 (1988) [1] as "the extent to which a product can be used by the target users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use". Authentication mechanisms impose to users an ancillary task (to identify to the system), which certainly is not the reason why the user is using the system. Authentication takes times, reduces performance and requires from users to memorize additional information on how to log in to the system. It might cause stress and dissatisfaction especially when authentication errors occur. We cannot objectively assert that authentication mechanisms are per see usable, but users might accept to use them up to a certain level without introducing deviant behaviors that might jeopardize security.

Currently, we still know very little about the factors that affect the usability of authentication mechanisms for mobile devices. However, we suggest that the interaction technique (way of entering personal identification) and the security policies implemented as parameters might play a role. In order to investigate this problem, we have implemented a testbed environment for assessing three authentication mechanisms, namely: PIN code, Android Pattern Lock and Passface. This testbed was conceived as an application that is aimed at helping with the setup of usability testing [5] of authentication mechanisms on mobile devices. The testbed has two modes: a setup mode for allowing the setup of the parameters of the experimentation and, a running mode that is used to collect user feedback. The setup mode allows tuning security policies such as the number of trials allowed, the length of passwords, delay between user interactions, availability (or not) of feedback for the user, etc. The user interaction is recorded in the form of a log file that can capture precisely the time of user interactions (which is an important feature to assessing performance), errors and mistakes. User satisfaction is measured in the testbed using a SUS questionnaire [6]. The rest of the paper is organized as follows: section 2, introduces the three authentication mechanisms and the diversity of parameters we are allowed to tune in each implementation; section 3 describes the testbed, in particular the two modes of functioning (setup and running modes); and, lately, section 4, concludes this paper and gives an overview about future works.

2 Overview of Authentication Mechanisms

Hereafter we present the three authentication mechanisms that are most commonly used to identify users of smartphone: PIN code, Android Pattern Lock and Passface. As we shall see, each of these mechanisms implemented a different set of parameters that can be tuned and combined to settle a large set of security policies. It is also worthy of notice that these three authentication mechanisms are based on memorization of textual/graphical elements, which require some cognitive effort and are very prone to forgetting. Thus, reducing the amount of information to be recalled would ultimately improve the overall usability of the authentication mechanisms.

2.1 PIN Code (Personal Identification Number)

PIN is a special case of a password using number only. The original patent [7] dates back to 1966 and it became very well know from ATM machines. PIN was also adopted by smartphone makers who, in some cases extended the length of the PIN from 4 digits in the original specification up to 17 in the newest Android system. The following parameters can be tuned in PIN implementation:

- *Random numeric keypad*: specifies how numbers are placed on the keypad: in random order or as classic numeric keypad (by default).
- *Pin code size*: represents the number of digits that makes up the PIN code. The default is 4 digits.
- *Number of attempts*: defines the number of trials before the device blocks the user. The default is 3.
- *Input indicator*: provides visual feedback to user actions. There are 4 possible options:
  1. No indicator at all. User does see anything on the phone screen as she/he enters the PIN.
  2. Dots to fill. The system shows a set of little circles equal to the length of the PIN. As the user enters the PIN, the corresponding circle of the entered digit is filled;
  3. Appearing dots. As user enters the PIN, a dot appears on the phone screen.
  4. Show last digit entered. This option allows the user to see the last digit entered. When the subsequent digit is entered, the previous digit is replaced with a dot.

2.2 Pattern Lock

In the Pattern Lock, the user is required to connect dots in a predefined order. Whilst Pattern Lock has many security drawbacks as presented in [8], it is still widely used in mobile phone. The parameters that can be varied for the pattern lock are the following:

- *Number of rows*: is the number of points/nodes laid horizontally on the screen. Default is 3.
- *Number of columns*: is the number of points/nodes laid down vertically. The default is 3. Number of rows and columns determine the total number of possible patterns available.
- *Size of the pattern*: is the number of interconnected points/nodes to create a pattern.
- *Size of the points/nodes*: is the size of the circles used to indicate points/nodes on the screen.
- *Number of attempts*: is the number of failures accepted when drawing the pattern before the phone blocks the user. The default is 3.
- *Vibration*: when this parameter is enabled, the phone vibrates as the user draws the pattern.
- *Stealth*: if this is enabled, the schematic plot of the pattern will be invisible on the phone screen.

2.3 Passface

Passface is a typical example of recognition-based systems that relies on user skill for face recognition [1]. The original implementation relies on human faces but many variants include other types of images. The Passfaces parameters include the following:

- *Number of tiles*: is the number photos/images displayed in a grid. Four options are available: 9 (3x3 grid), 12 (4x3 grid), 15 (5x3 grid), and 18 (6x3). The default is 9.
- *Photo Types*: it might be faces, animals, flowers, places, or other sets. The default is the faces.
- *Size of the Passfaces code*: is the number of photos that make up the password. The default is 5.

- *Number of steps*: is the number of steps/rounds to complete a Passface. If the size of the Passface code is 4, then the image selection and authentication will be done in 4 steps.
- *Image shuffling*: is the re-arrangement of the photos on the grid each time the user authenticates such that the images do not have fixed position on the grid. Image shuffling is enabled by default. This makes the positions of the images really pseudo-random.
- *Use same image multiple times*: determines whether (or not) a user is allowed to use the same photo to compose a Passfaces code. By default, an image is used only once.

3 Testbed implementation

Our testbed is an Android app that simulates the three authentication mechanisms. The design and the implementation of the app is modular, so that it is possible to add as many other authentication mechanisms as needed in the future. This app features two modes: a setup mode and an experiment mode. These two modes correspond to the necessary steps for building a user testing experiment with users. Figure 1 illustrates the main screen of the app where we can distinguish the entries to the following features: *create settings*, which correspond to the setup mode; *run experiments*, which corresponds to the mode used for user testing; *generate and view setups as PDF*, allowing to create a snapshot of the parameters used in each experiment; *manage users ids,* used for creating unique ids for the user testing to protect participants identity; and, *delete setups*, for removing experimental data not longer in use. In addition to that, the apps implements a log file that is presented hereafter.

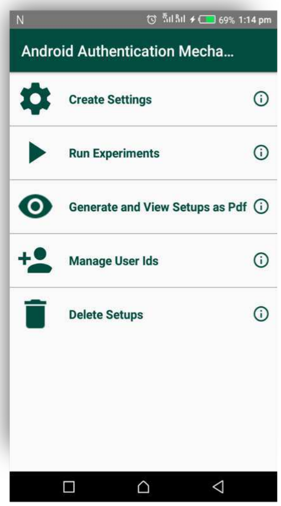


Figure 1: The main screen of the app

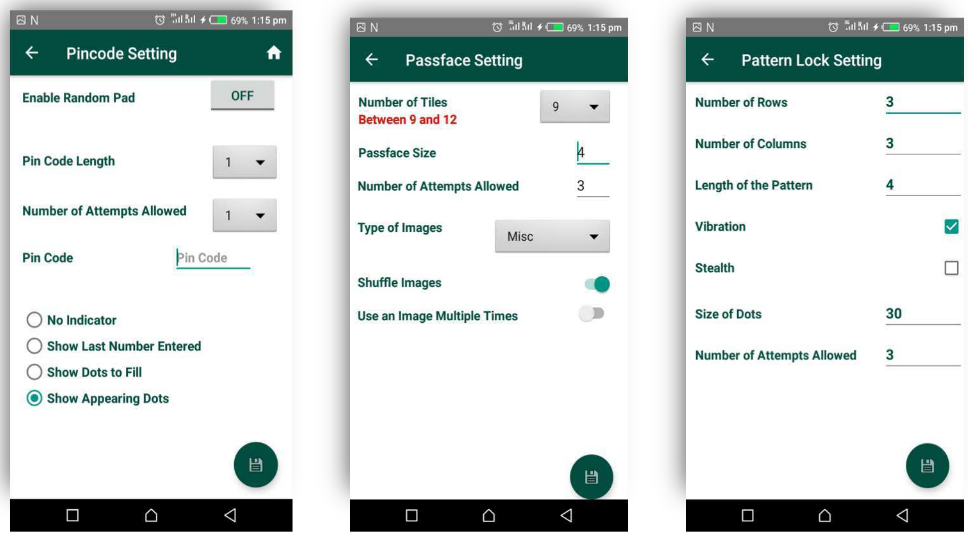
3.1 Setup mode

The main aim of the app is to conduct experiments by varying the various parameters associated with the authentication mechanisms. Therefore, the first step requires creating an evaluation setup with the configuration used in the user testing. So, using the appropriate entries, it is possible to configure the parameters for every authentication mechanism as shown in Figure 2. Every configuration must include a kind of password. The password is included as part of the configuration so that all users will use the same password in an experiment. This has the advantage of allowing a fair comparison of results assuming that the password is variable independent.

For the PIN code, the password is provided directly in the field *Pin code* as shown by Figure 2.a. For the Passface and Pattern Lock one more step is required, and we must use the screen as shown Figure 3 for entering the corresponding passwords.

For the Passface, we should tap the save button located on the bottom right of Figure 2.b. The app displays then the screen in Figure 3.a for the selection of the images. The images to be selected are in steps equal to the size of the Passfaces code as defined in Figure 2.b. After selection of the preferred images, theses image and the associated parameters set are then stored in the app database for use during the experimentation.

For the Pattern Lock, tapping on the save button located on the bottom right of Figure 2.c will open the screen as shown in Figure 3.b. After drawing the pattern, the button "TAKE SCREENSHOT" becomes active and allows the experimenter to take screen capture of the pattern. After taking the screen capture, the button "SAVE SETTING" becomes active so that the parameters set and the screen capture of the pattern can be saved in the app database.



Pincode Setting

Enable Random Pad: OFF

Pin Code Length: 1

Number of Attempts Allowed: 1

Pin Code: Pin Code

○ No Indicator
○ Show Last Number Entered
○ Show Dots to Fill
● Show Appearing Dots

Passface Setting

Number of Tiles: 9
Between 9 and 12

Passface Size: 4

Number of Attempts Allowed: 3

Type of Images: Misc

Shuffle Images: ●

Use an Image Multiple Times: ○

Pattern Lock Setting

Number of Rows: 3

Number of Columns: 3

Length of the Pattern: 4

Vibration ☑

Stealth □

Size of Dots: 30

Number of Attempts Allowed: 3

a) PIN code *b) Passface* *c) Pattern Lock*

Figure 2: Setup for parameters of the three authentication mechanisms: a) PIN, b) Passface, and c) Pattern Lock.

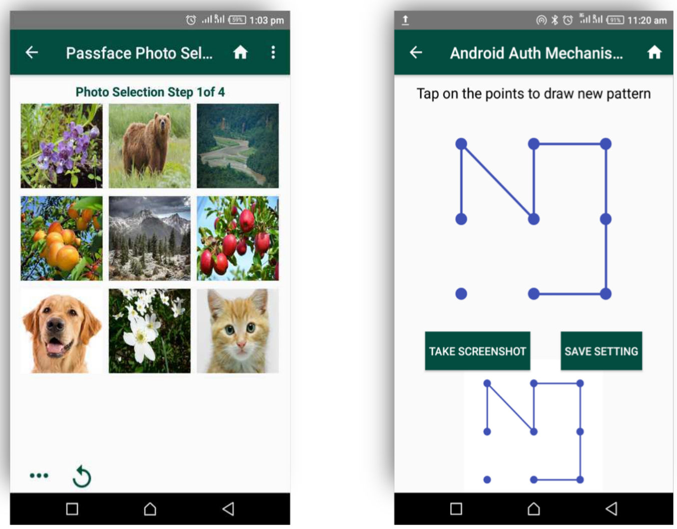
3.2 Running Mode

The goal of the running mode is to launch experiments using predefined configurations. The running mode is accessible from the option "Run experiment" on the main screen (see Figure 1) that leads to the screen shown in Figure 4.a, which presents the list of authentication mechanisms available. By selecting item in that list (Pattern Lock in this example), we move to the list of predefined configurations as shown in Figure 4.b. Once the configuration is selected, the application assigns an ID to the user who will perform the experiment (Figure 4.c). Identifying the users in this way allows preserving the identity of the real participants.

Figure 5 shows the screens used in the next steps of the evaluations. These screens are meant to be used by the user running the experiment. At first (Figure 5.a) the authentication mechanism is displayed; then the corresponding results follow with success (Figure 5.b) or fail (Figure 5.c).

In order to facilitate the experiment, the app allows the experimenter to generate the setups as pdf files so they can be printed and used during the experiment. This can be done by selecting the option

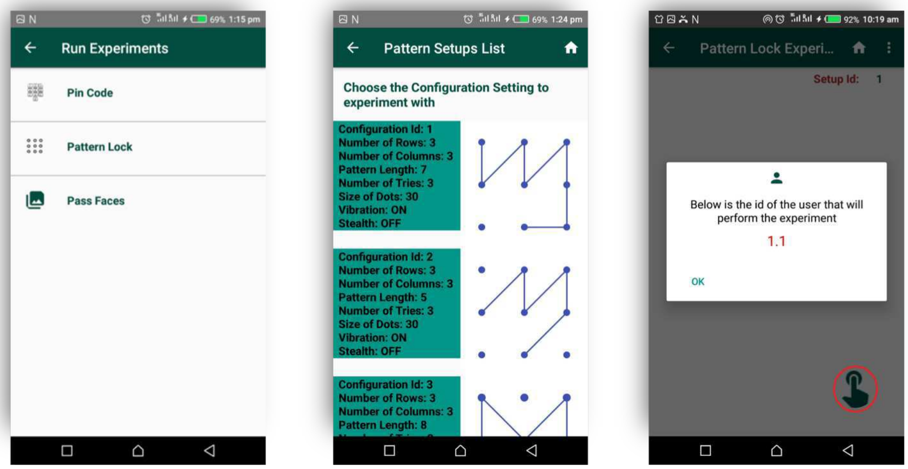
“*Generate and view setups as PDF”* from the main screen (see Figure 1). Having a printed version of the configuration is particularly useful to show the users the password they are going to use during the test. We will typically give it printed to the user along with the mobile device that will be used in the test.



Tap on the points to draw new pattern

a) Passface *b) Pattern Lock*

Figure 3: Entering a Passface password (a) and Pattern Lock (b).



Choose the Configuration Setting to experiment with

Configuration Id: 1
Number of Rows: 3
Number of Columns: 3
Pattern Length: 7
Number of Tries: 3
Size of Dots: 30
Vibration: ON
Stealth: OFF

Configuration Id: 2
Number of Rows: 3
Number of Columns: 3
Pattern Length: 5
Number of Tries: 3
Size of Dots: 30
Vibration: ON
Stealth: OFF

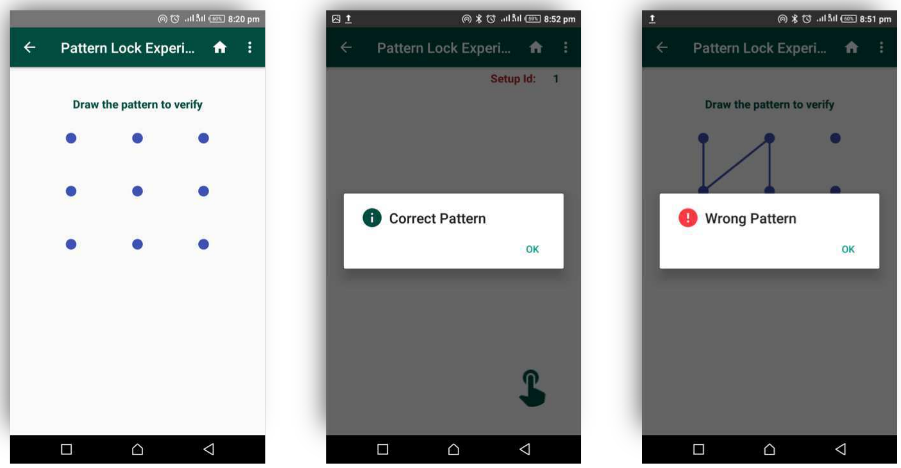
Configuration Id: 3
Number of Rows: 3
Number of Columns: 3
Pattern Length: 8

Below is the id of the user that will perform the experiment

1.1

a) Authentication mechanisms b) List of configurations available. c) User ID.

Figure 4: Main screens in running mode used by evaluator.



Correct Pattern

Wrong Pattern

a) Authentication mechanism b) Success c) Fail.

Figure 5: Main screens used by the user in the user testing.

3.3 Log Files

The app records the actions of the user during the experiments and stores this data as csv file. The app creates two folders: `Android Auth Mechs Log Files` and `Android Auth Mechs Setups PDFs`. The files `pattern_logs.csv`, `pincode_logs.csv`, and `passface_logs.csv` are the log files for Pattern lock, PIN code, and Passfaces authentication schemes respectively. These files are kept in `Android Auth Mechs Log Files`. All the csv files have the same pro form as illustrated by Table 1 below.

Config Id	User Id	User Actions	Attempt	Time	Date

Table 1: The pro forma for the csv log file for the 3 authentication mechanisms

`Config Id` is a unique identifier for a configuration setup. It is used to identify the configuration for a given experiment because there will be many configurations to experiment with. `User Id` uniquely identifies the user that performs an experiment. It is also just for identification purpose and does not relate to any personal identity of the user. `User Actions` is a column that records all the actions of a user during authentication: information such as when the user starts, when she/he finishes, and all the intermediary actions. `Attempt` column is used to keep information about during which trial the user does those action. For example, some users might be able to authenticate during the first attempt, some during the second attempt and so on. Finally, the `Time` and `Date` columns keep the time and the date of the authentication respectively.

In order to recall the setup of the experiment, the app supports the export of setups as PDF files named as `passfaces_setups.pdf`, `pattern_setups.pdf`, and `pincode_setups.pdf`. These files are available in the `Android Auth Mechs Setups PDFs folder`.

3.4 Managing Setups

After completing an experiment, the app allows the experimenter to get rid of setups that are no longer needed. This feature is also useful in case of mistakes when creating the setup. The management of setups is available from the main screen (see Figure 1). The option “Delete Setups” gives the list of available configurations that can be deleted according to the needs. Deleting a configuration does not delete the corresponding date from the log files.

4 Conclusion

In this work, we presented a mobile app that can be used as a testbed for assessing suitable configurations for authentication mechanisms. This testbed might have multiple applications. One practical scenario, would be to assess how users behave when using a specific authentication mechanism; in particular, users are not the same and cultural and personal traits might make people more or less keen to adopt more strict security measures.

However, the ultimate goal of this testbed is to help to automate user testing of authentication mechanisms so that we can start to investigate trade-offs between security and usability. Using this tool, we offer an opportunity for researchers to discover the impact of varying the parameters associated with these three authentication schemes in order to find the best acceptable thread-off between security and usability. To the best of our knowledge, there is no similar tool to our testbed.

For now, the application has been used as a proof of concept and tested with colleagues and students. In future work, we will focus on running large scale experiments.

The tool is freely available so that it can be used by the community of researchers interested in usability and security of authentication mechanisms.

References

[1] ISO 9241-11 (1998) Ergonomic requirements for office work with visual display terminals Part 11: Guidance on Usability. This standard has been revised by the ISO 9241-171:2008 Ergonomics of human-system interaction--Part 171: Guidance on software accessibility.

[2] Marcin Rogowski, Khalid Saeed, Mariusz Rybnik, Marek Tabedzki, Marcin Adamski. User Authentication for Mobile Devices. Khalid Saeed; Rituparna Chaki; Agostino Cortesi; Slawomir Wierzchoń. 12th International Conference on Information Systems and Industrial Management, Sep 2013, Krakow, Poland. Springer, Lecture Notes in Computer Science, LNCS-8104, pp.47-58, 2013, Computer Information Systems and Industrial Management.

[3] Jonathan Grudin, “Social Evaluation of User Interfaces. Who Does the Work and Who Gets the Benefit?” in H-J Bullinger and B. Shackel (eds.), Proceedings of INTERACT 1987 IFIP Conference on Human Computer Interaction (Elsevier,1987), 805–811.

[4] Karen Renaud. Evaluating authentication mechanisms (Chapter Six). Security and usability. O’Reilly Media, pages 103-128.

[5] Jeffrey Rubin and Dana Chisnell. Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests. Wiley Publishing, Inc. 2008. 384 pages. ISBN-13: 978-0470185483.

[6] John Brooke. 2013. SUS: a retrospective. J. Usability Studies 8, 2 (February 2013), 29-40.

[7] Ivan, A., Goodfellow, J.: Improvements in or relating to Customer-Operated Dispensing Systems. UK Patent #GB1197183. doi:10.1049/el:19650200 (1966).

[8] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge attacks on smartphone touch screens. In Proceedings of the 4th USENIX conference on Offensive technologies (WOOT'10). USENIX Association, Berkeley, CA, USA, 1-7.

[9] S Brostoff and A Sasse. Are passfaces more usable than passwords? a field trial investigation. In S. McDonald, editor, People and Computers XIV - Usability or Else! Proceedings of HCI 2000, pages 405–424. Springer, 2000.

Using Early Warning Score for vital signs analysis in *IoT* healthcare environment.

David Viana[1], Paulo Cunha[2], Odorico Monteiro[3], and Mauro Oliveira[1]

[1] IFCE - Instituto Federal de Ciência e Tecnologia do Ceará, Fortaleza, Ceará, Brasil
david.viana@ppgcc.ifce.edu.br
amauroboliveira@gmail.com
[2] UFC - Universidade Federal de Pernanbuco, Recife, Pernanbuco, Brasil
prfc@cin.ufpe.br
[3] UFC - Universidade Federal do Ceará, Fortaleza, Ceará, Brasil
odorico@ufc.br

Abstract

The ability to monitor vital signs in a hospital environment can be improved by information technology, specifically by IoT for healthcare. This technology allows services ranging from monitoring and analysis of vital signs in various environments and times of everyday life. This paper presents patient scenarios associated with data on heart rate, respiratory rate, blood pressure and peripheral oxygen saturation. By monitoring these data it is possible to calculate the risk score using the EWS (Early Warning Score), assisting health teams, reducing intervention times and improving data accuracy. The results obtained in this study demonstrate that individual monitoring and risk analysis, in hospital or other settings, besides improving the quality of care, can reduce the time to identify which patients are at risk, increasing the accuracy of the monitored signals.

1 Introduction

he Internet of Things (IoT) is an emerging technology that can modify the way we know the industry, can be applied in several areas and help solve various problems [15]. To reinforce the emergence of this technology, forecasts predict that by 2020 there will be more than 40 billion connected devices, [8, 11].

This transformation is caused by the constant technological development of this area. According to [10] mobile health technologies can modify clinical intervention especially in the care of the elderly with chronic diseases and in the monitoring of NCDs such as cancer, diabetes, cardiovascular diseases and respiratory [14]. The WHO (World Health Organization) stands for 2025 the elderly population will be 14.8% of the world's population. This problem, along with NCDs, will be challenges to health development in the 21st century [14]. The growth of IoT applications is a real demand. Healthcare devices for monitoring vital signs based on conventional IoT have primary tasks such as gateways for receiving and transmitting data, reinforcing the perception of the possibility of Fog Computing. The results presented by [2] demonstrate that automated monitoring of individuals improves the accuracy of the data and the earlier one perceives the deterioration of individuals, the shorter the time for activation of the Rapid Response Team (RRT). This activation is based on risk values calculated through the pre-defined EWS scale (early warning score). In [2] it is verified, due to the computerization, that there are improvements in the accuracy and the time of perception of deterioration of the individual. Already [12] presents a team dedicated to improve without automation the accuracy of data and vital signs. Thus, supporting the results of [2] in the work of [12], it is perceived that it is very difficult to maintain the precision in the acquisition of these signals, since the qualitative factors are those that most affect the work of the team. An IoT-based system can provide a monitoring service and alerts can be efficient when using protocols such as EWS and/or EPFC (Escalation Protocol Flow Chart), which describes the procedures to be performed. The objective of this work is to use the use of these two health protocols and apply them in simulations to save energy and transmissions to the cloud.

In section two, presents concepts of healthcare alerts (EWS and EPFC). Section three will show concepts and scenarios of patients in attendment. Section four presents methodology, database, and software used. Section five shows related works and relevance of the proposed here. Section six presents the results, at section seven discussion and section eight conclusion and future works.

2 Healthcare alerts

EWS is a system that calculates values of vital signs measured and recorded by the nursing team. The objective is to identify the deterioration of the individual from the following vital signs: Pulse, Blood Pressure, Respiratory Rate and Temperature [1].

Another approach to the EWS is the ViEWS which, in addition to all of the vital signs mentioned above, includes observation of the whole and verifies the individual's breathing with the help of artificial oxygen and voice response alert information, pain response and/or lack of response. Table 1 shows the signal boundaries and their score.

Score	3	2	1	0	1	2	3
Respiratory rate (breaths/min)	<=8		9–11	12–20		21–24	>=25
SpO2(%)	<=91	92–93	94–95	>=96			
Temperature (C)	<=35		35.1–36	36.1–38	38.1–39	>=39	
Systolic BP(mmHg)	<=90	91–100	101–110	111–249	>=250		
Heart rate(bpm)		<=40	41–45	51–90	91–110	111–130	>=131

AVPU							Verbal(V)
							Pain(P)
							Unresponsive(U)

Inspired O2 FiO2				Air			Any O2

Table 1: Risk scale EWS/ViEWS - Adapted from [1].

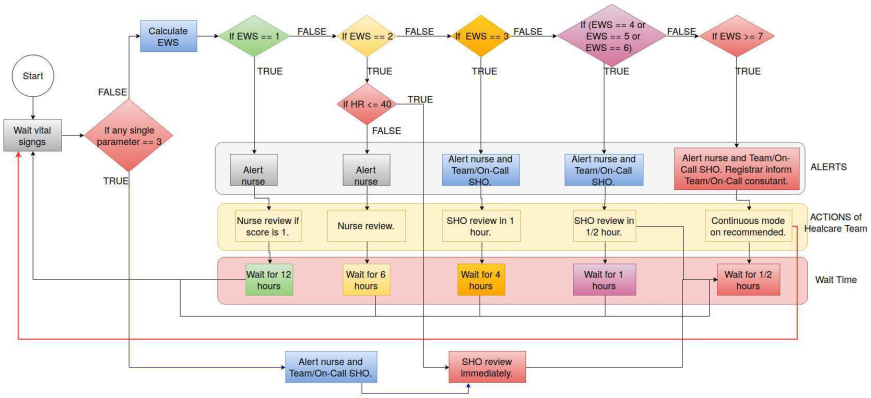


Figure 1: Flow chart of Escalation protocol EWS - Adapted from [1].

3 Monitoring scenarios

The purpose of the scenarios in this work is to organize/contextualize the use of day-to-day sensors of people who need some care, collecting, measuring, storing, inferring intelligence and analyzing risks to promote the health of the individual [10]. Thus, in all these scenarios people previously use in their day-to-day some kind of sensor of the type bracelet capturing some vital signs, similarly as in [9], which suggests capturing pulse in beats per minute, spo2 (oxygen saturation) and temperature.

Individual on the street: in this scenario the patient can be monitored as he presented the work [9]: It shows through a bracelet the capture of the pulse, spo2 and temperature. The mobile application sends the vital signs to the cloud, where an emergency service can be triggered in the event of a person's accident, fall, or malaise. In this scenario, there is a stand-alone concept. Therefore, it is necessary to use dew computing and intelligence on the context so that unimportant messages are not transmitted to the cloud. At an opportune moment, the individual's historical information is sent to the cloud or at a relevant moment as in an accident or fall event.

Individual in ready care: prompt care is the case where the patient has a complaint and goes to a doctor on call who evaluates it. The physician can access the information of the last days reported by the individual, verify if their complaints are related to the monitored vital signs, medicines and electronic medical record. In this scenario, the stored data is characterized by centrality and an intelligence can analyze the data and show possible indications of diagnoses. It can be said that artificial intelligence, ontologies and data mining would help as in the study [5] and can infer more information.

Individual in the observation room during emergency care: in the observation room the person may be connected to more sensors and have more vital signs observed for evaluation and follow-up by the health team [9]. In this case, personal data and vital signs can be placed in a context above the location and below the cloud, a fog context. The person begins to be monitored and evaluated by his/her vital signs through a context that concentrates the data before sending to the cloud. Although a context of intelligence, datamining or ontologies is again similar to the work of [5], the EWS analysis can also be taken into account.

Individual hospitalized in a hospital bed: hospital admission chart requires a lot of care and procedures already in the hospital. The use of sensors at this time is almost mandatory, however, there are several levels of monitoring [10]. In this case, Dew, Fog and Cloud computing approaches may be required, in addition to the risk analysis approach using the EWS.

Individual at home: in this scenario, the patient may have several situations, here they were divided into 3: **total individual dependent on caregivers, restricted to bed and monitored** - this case resembles that of the individual in the ward or hospitalized; **individual not bedridden and partially dependent on the caregiver for support in the necessities of daily living -** here, the scenario may be similar to that of the individual who moves but needs support from a second person to carry out their activities of daily living; **independent person -** in this scenario, the individual can be compared to the individual on the street.

4 Methodology

4.1 Data and software used

A risk comparison was performed using vital signs values from the maximum and minimum limits, according to the literature, in comparison to the calculation of the EWS risk score.

According to [4], when the temperature of an adult is above 37.5 ° C, the individual is considered to have a fever, and below 35 ° C, characterizes hypothermia. For the data of cardiac arrhythmia problems, the following interval was used: values above 100 bpm and below 60 bpm.

For blood oxygen saturation levels, it should be equal to or above 95%, so any value below should be alarming [4]. For systolic blood pressure, normal values should be 80 to 120 mmHg and diastolic values of 60 to 80 mmHg. For the respiratory rate, the values are between 14 and 20 breaths per minute. In this work the physionet/MIMIC database was used, which has several monitored vital signs of individuals in the Intensive Care Unit (ICU). Only subjects with the following vital signs were used for a period of approximately 12 hours per second: respiratory rate, heart rate, SpO2, and systolic blood pressure. The number of individuals on this basis with these vital signs totaled 36.

The Octave version 4.2.2 was used to compare the data and to initially perceive the differences or similarities between the monitoring of the patients using the parameters of the literature and using the EWS scale. Thus, three functions have been created: The first (normalClassification), returns true or false for each signal presented if it were with parameters outside of normal. The second (ewsClassification) returns true for any of the risk scores above or equal to 1, or false for risk 0. The third (riskLevel) calculates the risk rating of each displayed signal that returns values from 0 to 5, where 0 represents the Patient without risk and from 1 to 5 represents the risk classified according to the EWS system.

To reduce the number of transmissions of the signals to the cloud and to decrease the signals that can be measured by some type of fault or discrepant values, the calculation of the arithmetic mean of risk was used for a period of 60 samples, in this case, for 60 seconds. Since EWS scale times allow monitoring ranging from 30 minutes to 12 hours, this period has been adopted here.

4.2 Network simulation

To simulate the data that travels in the network, the CORE (Common Open Research Emulator) software and Wireshark were used to verify/measure the traffic statistics of this simulation.

In the simulation, to reduce the simulation time the data were transmitted every 0.1 seconds. Thus, each sensor node carries vital sign data (respiratory rate, spo2, systolic blood pressure, and heart rate) of each person in the MIMIC database. Then each node processes the risk and transmits it to the centralizing node. This stores 60 samples of each person, calculates the arithmetic mean and transmits the risk to the cloud. The following messages are set to send the individual's signals and their risks respectively.

Message of vital signs: {"bmp":"valor (max 10 bytes)", "spo2":"valor (max 10 bytes)", "rr":"valor (max 10 bytes)", "systo":"valor (max 10 bytes)", "id":"valor (max 10 bytes)"}.

Message of risk: {"id": "valor (max 10 bytes)", "risk": "value (max 2 bytes)"}

5 Related work and motivation

Work [7] used a mesh topology network for communication between devices to send the monitored temperature. While this work will use a TCP/IP network and a client-server architecture.

A Fog architecture is proposed to process signals through FPGA with a mesh layer to aggregate data before processing them in the Fog layer. In this research the idea of Fog will also be used to try to reduce the flow of data transmitted based on the risk of the patient.

The use of NEWS (National Early Warning Score) was proposed in the work of [6] to assess the patient's risk situation, together with a proposal of evaluation using the Fuzzy Inference

System (FIS). However, signaling thresholds and health procedures using EWS are already defined and documented in consolidated health monitoring procedures, so it is proposed here to use this health protocol to determine the patient's degree of risk.

In the work of [15], a service-oriented IoT architecture proposal is presented and compared to SOA, SOA-IoT, with arguments that both SOA and IoT would be to promote network and service heterogeneity. The proposal of heterogeneity here is to use the EWS to redefine what data will be transmitted and what data will be marked to decrease the flow, addressing the quality of service of the network.

A system was proposed and tested to monitor the vital signs of patients, their requests for care, and the moment the health team responds to the request for care. Thus, in the continuation of this work, as mentioned previously, a risk classification of EWS vital signs will be used.

6 Results

Figure 2, in blue, represents the percentage of vital signs that puts each individual at risk according to the following parameters and intervals: Respiratory rate: greater than 20 or less than 14 breaths per minute; Oxygen blood saturation - SpO2: less than 95%; Systolic blood pressure: less than 80 or greater than 120 mmHg; Heart rate: less than 60 or greater than 100 beats per minute. When the patient encounters all normal signs the risk is taken as zero, so the above result shows 12 initial monitoring hours using these intervals.

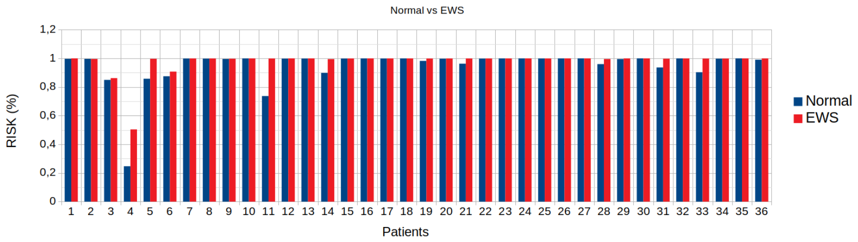


Figure 2: Classification of signs of patients evaluating the signs by ”normal” classification and using EWS.

Figure 2, in red, represents the percentage of vital signs that put the individual at risk above 0. Individuals 3, 4 and 5 are those with the highest risk percentage with a value of 0, while the others are practically 100% risk. These results demonstrate that data from the MIMIC database, with or without the EWS scale, are mostly at critical levels above 0 and in this case confirm the critical state of those persons hospitalized in the ICU.

Figure 3 represents the percentage amount of vital signs for the risk rating ranging from 0 to 5 for each user. It is clear that when using this approach, because the EWS can evident urgent patients, health team can adopt monitoring periods and what level of risk should alert them by improving the quality of care since it is essential for the recovery of the individual [1].

In Figure 4 (left), represents the risk classification of users 1, 2, 3, 4 and 5 in the 12-hour interval or 43,200 seconds. Figure 4 (right) represents the average risk in the 60-second period. It can be seen that this average can represent the signal scores per second, reducing noisy points and discrepant signals.

Figure 5 shows the simulation of part of the data of the first 5 patients through the CORE simulation using the Dew and Fog computing paradigms. The sensor nodes calculate the EWS

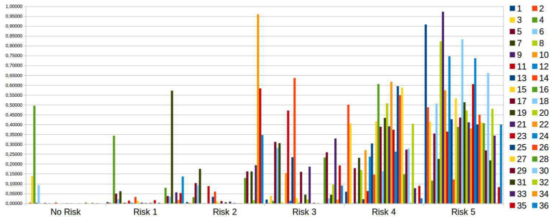


Figure 3: Risk classification according to each level for each individual.

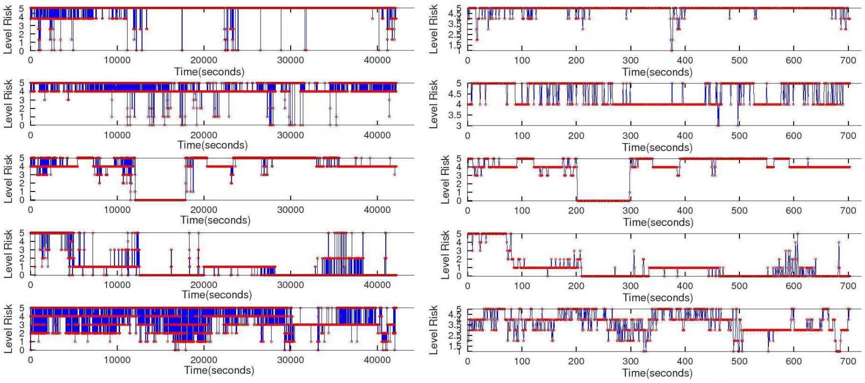


Figure 4: Left - EWS classification of users 1, 2, 3, 4 and 5 over time. Right - Risk classification by arithmetic mean at 60-second intervals.

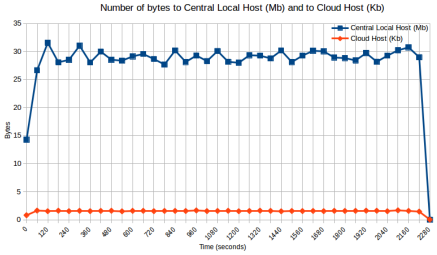


Figure 5: Simulation of traffic using CORE software

risk and send it to the central node in the local network. Lastly, it stores 60 of these values for each patient and then calculates the average for the period, sending the average risk to the cloud.

7 Discussion

It is relevant that using the individual risk classification according to the literature presented, even for non-ICU patients, differs from the EWS classification. In general terms, it is perceived that using only the classification, risk or risk-free, both for the first approach and for the second one generates a false interpretation of the risk of the individual [1]. Thus, when the

EWS risk classification is used through the various levels, the on-site observation period can be verified/alerted by the nursing team. However, through computer systems such as IoT, the health team can be warned, or can access at any time the data of the people monitored.

The individuals analyzed have risk levels practically at each of the six presented levels. This means that when monitoring the risk through the IoT/EWS architecture, the time of intervention by the health team can be efficiently reduced. It can also be determined the periods in which the team would need to intervene, optimizing the work of the team and improving the performance established in the protocol, or even the need to wait, but due to the real time service and the system inference. Therefore, the effectiveness of the health team, which [2] impacts on accuracy and quality of service, even with dedication and commitment, would not be a problem simply by automated monitoring [12], and by using information to improve clinical intervention [10].

In the Fog computing paradigm, where the data travels mainly in the local network, the data would be every second traveling in the network until the centralizing node, therefore, the bandwidth should be enough to be able to offer an efficient service of monitoring be it in real time or not, which should alert the health team to the states of individuals. In the Fog computing approach, as in [3], there are some network properties such as, bandwidth, availability, delay, losses that may be relevant, so network services can be affected. It is then understood that in the context Fog can be used to only send data to the cloud, or to a central of situation only the information relevant to the care of patients with a high degree of risk, thus, reducing the data flow on the network. And the other approach, as in this paper, may be to use the arithmetic mean of a given period that may well represent the individual's level of risk. It is noteworthy that using an arithmetic mean is an approach that reduces the number of transmissions per second and yet well characterizes the risk level of individuals (see Figure 4).

In the Dew computing paradigm, using the arithmetic mean at each node, it is possible to decrease packets trafficked in the local network, while the centralizing node only processes the level of risk that the health team will use to generate alerts in the cloud service [13]. This demonstrates that this approach unlike the previous approach can have an impact on data transmission, bandwidth usage, reduced data traffic to both the local network and the cloud. Therefore, monitoring the vital signs not only of the people in the ICU, but also in any of the scenarios described in section 3, is a way of seeking efficiency of the IoT services according to [15] and [10].

8 Conclusion

To use EWS risk scale in the decision to transmit individuals' data can reduce network traffic according to the level of risk that the health team selects and when calculating the arithmetic mean, a very significant reduction can be achieved, since the time periods of the EWS scale allow monitoring from 30 minutes to 12 hours. Therefore, through a computer system this can be monitored at any time, however, there is a need for containment, in several ways, in this case was decreased when transmitting this information. This is because Dew and/or Fog paradigms can be explored. It is therefore noticeable that the simplicity of this service and this architecture should be tested with more devices performing network performance tests. Another important observation is to also research on other risk protocols, making a comparison between them and finally in future works to provide QoS on the data using the risk levels to label the transmitted packets. This approach allows to define efficient periods of visit of the health team, allows to generate alerts at any moment, as well as to establish standards to define where the best moment for the team to act using artificial intelligence, data mining or ontology.

References

[1] Bronwyn Avard, Heather McKay, Nicole Slater, Paul Lamberth, Kathryn Daveson, and Mogen Mitchell. Training Manual for The National Early Warning Score and associated Education Programme. *Health Service Executive*, (June), 2011.

[2] Rinaldo Bellomo, Michael Ackerman, Michael Bailey, Richard Beale, Greg Clancy, Valerie Danesh, Andreas Hvarfner, Edgar Jimenez, David Konrad, Michele Lecardo, Kimberly S. Pattee, Josephine Ritchie, Kathie Sherman, and Peter Tangkau. A controlled trial of electronic automated advisory vital signs monitoring in general hospital wards. *Critical Care Medicine*, 40(8):2349–2361, 2012.

[3] Luca Cerina, Sara Notargiacomo, Matteo GrecoLuca Paccanit, and Marco Domenico Santambrogio. A fog-computing architecture for preventive healthcare and assisted living in smart ambients. *2017 IEEE 3rd International Forum on Research and Technologies for Society and Industry (RTSI)*, pages 1–6, 2017.

[4] Ministério da Saúde, Secretaria de Gestão do Trabalho e da Educação na Saúde, Departamento de Gestão da Educação na S, and Aúde. *Profissionalização de Auxiliares de Enfermagem - Fundamentos de Enfermagem 3.* 2003.

[5] Renato Freitas, Cleilton Rocha, Oton Braga, Gabriel Lopes, Odorico Monteiro, and Mauro Oliveira. Using Linked Data in the Data Integration for Maternal and Infant Death Risk of the SUS in the GISSA Project. *Proceedings of the 23rd Brazillian Symposium on Multimedia and the Web - WebMedia '17*, pages 193–196, 2017.

[6] Carol Habib, Abdallah Makhoul, Rony Darazi, and Raphaël Couturier. Multisensor Data Fusion for Patient Risk Level Determination and Decision-support in Wireless Body Sensor Networks. *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems - MSWiM '16*, pages 221–224, 2016.

[7] Ravi Kishore Kodali, Govinda Swamy, and Boppana Lakshmi. An implementation of IoT for healthcare. *2015 IEEE Recent Advances in Intelligent Computational Systems, RAICS 2015*, (December):411–416, 2016.

[8] B. V. S. Krishna and T. Gnanasekaran. A systematic study of security issues in internet-of-things (iot). pages 107–111, Feb 2017.

[9] Vitor Lopes, Emilson Rocha, Eliezio Queiroz, Nicodemos Freitas, David Viana, and Mauro Oliveira. VITESSE - more intelligence with emerging technologies for health systems. *2016 7th International Conference on the Network of the Future (NOF)*, pages 1–3, 2016.

[10] Pradeep Ray, Politecnico Milano, and Aura Ganz. mHealth Technologies for Chronic Diseases and Elders : A Systematic Review mHealth Technologies for Chronic Diseases and Elders : A Systematic Review. 31(September):6–18, 2013.

[11] Melnik Sergey, Smirnov Nikolay, and Erokhin Sergey. Cyber security concept for Internet of Everything (IoE). *2017 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SINKHROINFO 2017*, 2017.

[12] Cristiane Chagas Teixeira, Rafaela Peres Boaventura, Adrielle Cristina Silva Souza, Thatianny Tanferri de Brito Paranaguá, Ana Lúcia Queiroz Bezerra, Maria Márcia Bachion, and Virginia Visconde Brasil. Vital Signs Measurement: an Indicator of Safe Care Delivered To Elderly Patients. *Texto & Contexto - Enfermagem*, 24(4):1071–1078, 2015.

[13] Y. Wang. The initial definition of dew computing., November 2015.

[14] WHO. Global status report on noncommunicable diseases 2014. *World Health*, page 176, 2014.

[15] L. D. Xu, W. He, and S. Li. Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4):2233–2243, Nov 2014.

A Metric for Resource Usage Evaluation in Cloud Computing Environments

Tiago da Silva Nascimento[2], Emanuel Coutinho[1,3,5], Carla Ilane Bezerra[3,5], and José Neuman de Souza[4,5]

[1] IBITURUNA – Research Group of Cloud Computing and Systems
[2] Federal University of Bahia, Salvador (UFBA), Bahia, Brazil
[3] Campus Quixadá – Federal University of Ceará (UFC) – Quixadá, Brazil
[4] Master and Doctorate in Computer Science (MDCC)
[5] Federal University of Ceará (UFC) – Fortaleza – Ceará – Brazil
tiagodasnascimento@gmail.com, emanuel@virtual.ufc.br, carlailane@ufc.br, neuman@ufc.br

Abstract

Cloud Computing (CC) has become a subject of considerable research in the scientific and industrial communities, as well as other technologies. Although there are several studies and recent developments stating CC is still in the process of evolution and increasingly new technologies are emerging that can be added to it, such as Software Defined Networks (SDN) and Network Functions Virtualization (NFV). The quality evaluation of these technologies tends to become increasingly important, and this directly impacts the users. Due to the emergence of CC, SDN and NFV technologies, and the fact that they are highly related, it was necessary to evaluate the quality of these environments in an integrated way. This work proposes a metric for the quality evaluation of integrated environments.

1 Introduction

Over the years, Cloud Computing (CC) has become a subject of considerable research in the scientific and industrial communities, as it represents a new era for the availability and use of Information Technology services through the Internet [15]. The cloud computing paradigm is based on a usage-based payment model, and suggests the integration of various technology models to provide hardware infrastructure, development platforms, and applications such as on-demand services [7].

Although there are several studies and recent developments, CC is still in the process of evolution and increasingly new technologies are emerging that can be added to it [1]. This is the case of Software Defined Networks and Network Functions Virtualization.

Software Defined Networking (SDN) represents a paradigm that promises to change the state of traditional IP (Internet Protocol) networks, which are considered complex and difficult to manage, because they have the control plane and the data plane grouped into the network devices. SDN breaks vertical integration with the separation of these planes (control and data). In this way, the control functionality is removed from devices, which become simple packet forwarding elements [11].

Network Functions Virtualization (NFV) emerged as a solution to the challenges faced by telecom service providers, as it leads to virtualization technology to provide a new way to design, deploy, and manage network services [2]. NFV disassociates the Network Functions of the physical equipment where they are executed, which can lead to significant reductions in operating expenses (OPEX) and capital Expenses (CAPEX), in addition to promoting greater return and agility in the implementation of new services [13].

Cloud computing network infrastructure is shared with a number of independent entities. Therefore, network management is a challenge. In this context, SDN has highly valuable features for cloud computing systems, and also plays an important role in NFV technology infrastructure by making networks more flexible, dynamic and cost-effective, while simplifying the operational complexities [2].

With the great use of Information and Communication Technologies at all levels of human activity, the evaluation of the quality of these technologies tends to become increasingly important [8]. Thus, due to the emergence of CC, SDN and NFV technologies, and the fact that they are highly related, it was necessary to evaluate the quality of these environments in an integrated way. A quality evaluation can be performed by measuring the quality attributes of the technology in question [10].

In this context of cloud quality assessment, this work proposes a metric for the evaluation of the quality of integrated Cloud Computing, Network Defined by Software and Network Function Virtualization environments, with the main target audience being the researchers areas.

This work is still in progress, and therefore the experiments only used the environment of a computational hybrid cloud. This paper presents an initial idea of a metric to analyze the quality of the environment. It is also a way of knowing the used tool, to analyze its flexibility in the inclusion of new metrics. However, the environment did not use SDN or NFV resources, remaining for future work and application of the tool in these environments.

2 Related Work

[12] presented a proposal for a comprehensive quality model for assessing the quality of Software as a Service (SaaS) cloud services. Based on ISO/IEC 9126 [9], these authors identified characteristics, quality attributes and defined metrics to measure the quality of these attributes. This work does not make any practical application in a real environment of defined metrics and its quality assessment model is directed to a specific model of cloud computing (SaaS).

[16] proposed a quality model for cloud services called CLOUDQUAL, which specifies six quality assessment metrics that serve cloud services in general. In this work, the authors designed a case study involving three real-world storage clouds: Amazon S3, Microsoft Windows Azure Blob Storage (Azure Blob) and Aliyun Open Storage Service (Aliyun OSS). By the use of experimental results, the effectiveness of CLOUDQUAL was analyzed and its use for evaluating the quality of cloud services is feasible.

[14] performed a systematic mapping on the current state of the art of the proposed Web service quality models, using ISO/IEC 25010 [10] for articulation of the analysis. This work presented characteristics and attributes of quality, with the definitions most used in Web service quality models for these dimensions.

[5] proposed same metrics for elasticity evaluation in cloud environments, based on concepts from Physics and Microeconomics. This metrics could be used in some future work in SDN and NFV environments for evaluating the elasticity effects under different workloads.

The idea of these works was to discuss quality assessment for cloud computing environments, as well as aspects, characteristics and quality attributes. This is one of the ideas of our work.

3 Description of the Hybrid Cloud Environment

3.1 Testbed

The experiments used two different cloud computing environments: a private cloud and a public cloud. For the private cloud we used OpenNebula 3.8. All physical machines had 5 or 7 cores, 24 GB RAM, Linux Ubuntu Server 12.04 64-bit operating system and KVM hypervisor. Each virtual machine was created with 1 VCPU, 1 GB of RAM and Linux operating system Ubuntu Server 12.04 64 bit. For the public cloud, the Microsoft Azure platform was used, with instances created with standard type A1 (1 core and 1.75 GB of RAM) and Linux operating system Ubuntu Server 14.04 64 bit.

The experiments used a maximum of four virtual machines, varying the number of instances used in the private and public cloud, according to the design of the experiment. Apache Tomcat was used as web server, NGINX as load balancer and HTTPERF as workload generator. Figure 1 displays the used testbed, based on the architecture proposed in [4].

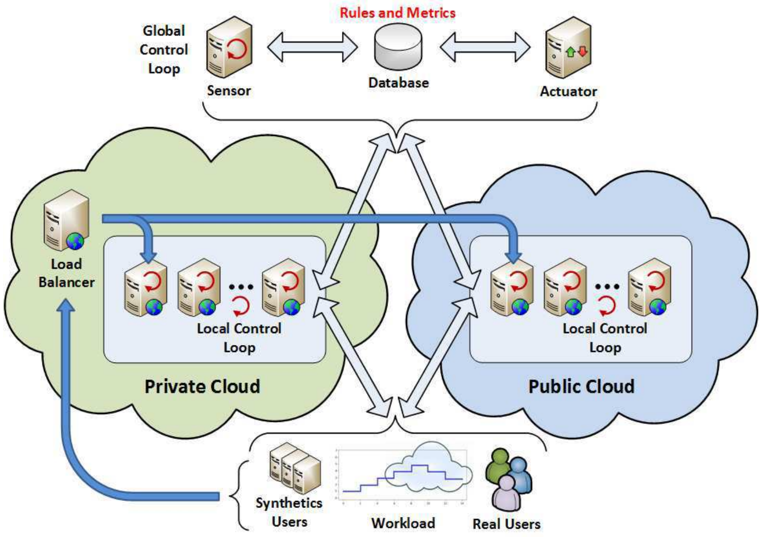


Figure 1: Autonomic architecture for elasticity in cloud computing using private and public clouds [4]

3.2 Workload

The workloads generated for the experiments were given by: requests forwarded directly to the load balancer virtual machine, generated by HTTPERF (with load of a multiplication of matrices) and by web browsers, distributed among the others virtual machines allocated; and requests executed directly on the virtual machines used by the infrastructure. Thus, competition for resources in a CC environment can be emulated [4]. Figure 2 represents the applied workload.

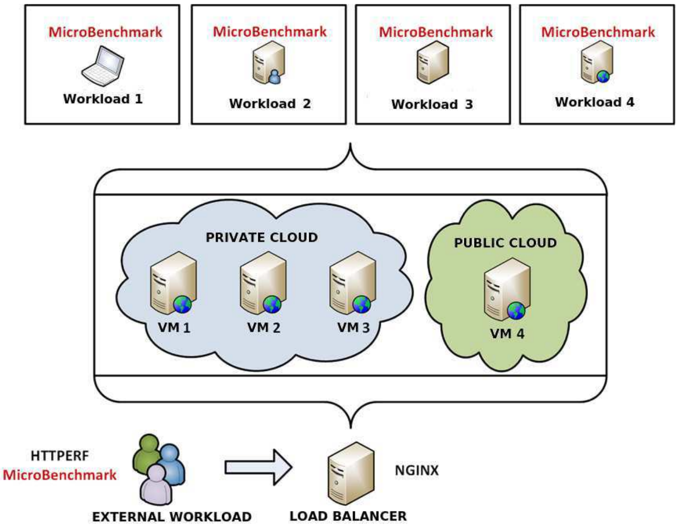


Figure 2: Workload applied to the infrastructure [6]

3.3 Metrics Analysis Support Tool

To assist in the visualization and analysis of the collected data, a tool was used that allows the generation of graphs for the various metrics collected from the environment resources [3] (Figure 3). This application was developed with Java programming language. It is based on the reading of text files, which contains information collected from the environment, such as CPU and memory usage, as well as application data such as response time for requests. The log files have their own structure read by the application. Examples of log files are: virtual machine allocation and average CPU consumption. These files are illustrated in Table 1 and Figure 4

File	**Structure**
Virtual Machine Allocation	Date of collection; Maintain (m), Increase (a) or Decrease (d); Number of allocated virtual machines
Average CPU consumption	Date of collection; Average percentage of CPU value in all virtual machines

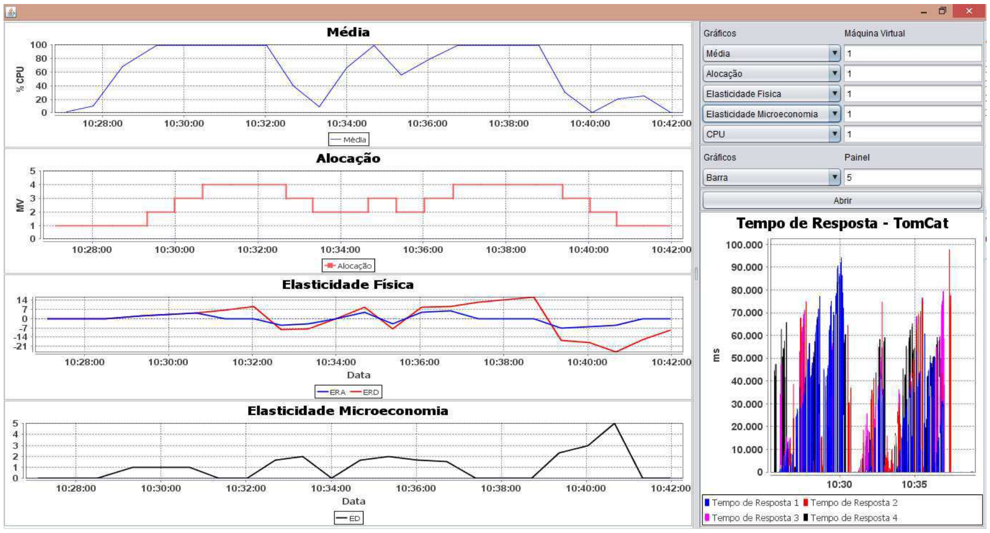
Table 1: Structure of the log files

3.4 Application of Metrics

For experiments performing, a metric of resource utilization was used. In addition to the resource utilization metric, the average CPU usage metric was used to aid in the evaluation of resource utilization. The following formula was used for the resource utilization metric:

$$R_u = \frac{R_a}{R_p} \tag{1}$$

Where R_u, R_a and R_p are equivalent to the used resources, allocated resources, and pre-allocated resources, respectively. In our experiments, we used virtual machines as resources.



Gráficos	Máquina Virtual
Média	1
Alocação	1
Elasticidade Física	1
Elasticidade Microeconomia	1
CPU	1

Gráficos	Painel
Barra	5

Figure 3: General screen of the application for metrics analysis [3]

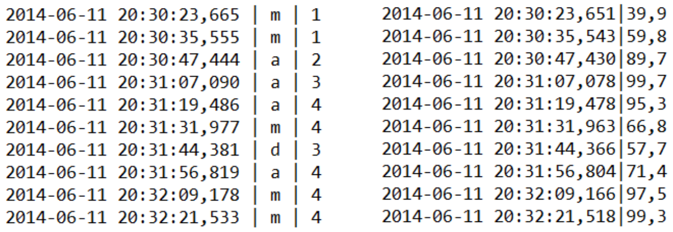

```
2014-06-11 20:30:23,665 | m | 1      2014-06-11 20:30:23,651|39,9
2014-06-11 20:30:35,555 | m | 1      2014-06-11 20:30:35,543|59,8
2014-06-11 20:30:47,444 | a | 2      2014-06-11 20:30:47,430|89,7
2014-06-11 20:31:07,090 | a | 3      2014-06-11 20:31:07,078|99,7
2014-06-11 20:31:19,486 | a | 4      2014-06-11 20:31:19,478|95,3
2014-06-11 20:31:31,977 | m | 4      2014-06-11 20:31:31,963|66,8
2014-06-11 20:31:44,381 | d | 3      2014-06-11 20:31:44,366|57,7
2014-06-11 20:31:56,819 | a | 4      2014-06-11 20:31:56,804|71,4
2014-06-11 20:32:09,178 | m | 4      2014-06-11 20:32:09,166|97,5
2014-06-11 20:32:21,533 | m | 4      2014-06-11 20:32:21,518|99,3
```

Figure 4: Excerpts from the log files for virtual machines allocation and average CPU utilization

The implementation of the resource utilization metric was basically due to the relationship of resource utilization data with the total sampling time. The CPU Average metric shows an average CPU utilization of the hybrid system completely. This metric was already implemented in the tool, as previously mentioned. In the same way, as the allocation of virtual machines.

4 Experiments

For the metrics application, we used the database of the experiments described in the following subsections (4.1 e 4.2), available in [6].

4.1 Experiment 1 - One Virtual Machine in the Private Cloud and One Virtual Machine in the Public Cloud

This experiment lasted 36min10s. Only two virtual machines were involved in this experiment: one in the private cloud and one in the public cloud. In this way, it was possible to verify if the designed infrastructure would provide resources of the two clouds, constituting a hybrid cloud, according to the necessity generated by the workload.

Figure 5 shows the graphs generated from the application of the Resource Utilization and CPU Average metrics, with the allocation of the virtual machines for complementary analysis.

From the analysis of the graph illustrated by Figure 5, it can be seen that the CPU utilization average varied between practically all points of the ordinate axis (% CPU), reaching points of use of 100%. From this information, it can be seen that many requests were occurring and there were few virtual machines to meet these requests. Relating the CPU Average graph to the Resource Usage chart, it can be noted that when the CPU reaches an average usage of approximately 80% the load balancer starts to allocate more resources, in which case it allocates another machine in the public cloud to aid in the processing of excess load.

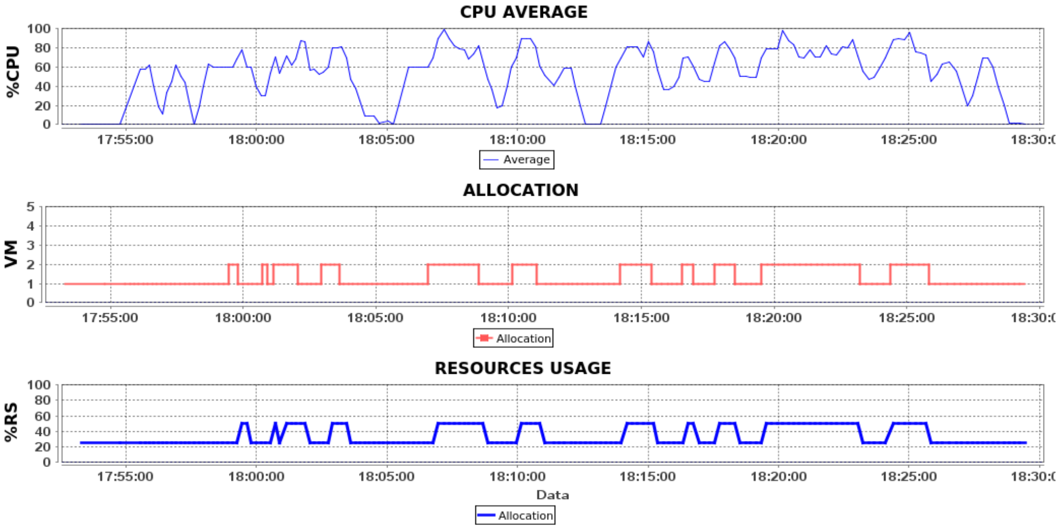


Figure 5: Experiment 1: One virtual machine in the private cloud and one virtual machine in the public cloud. CPU Average Usage, Virtual Machine Allocation and Resource Utilization graphics

4.2 Experiment 2 - Three Virtual Machines in the Private Cloud and One Virtual Machine in the Public Cloud

This experiment lasted 11min14s. Four virtual machines were involved in this experiment: three in the private cloud and one in the public cloud. Thus, it was possible to verify if the infrastructure performance would be impacted by the addition of a virtual machine from a public cloud, and whether the SLA (Service Level Agreement) would be maintained.

Figure 6 displays the graphs generated from the Resource Utilization and Average CPU metrics application. It also presents the allocation of virtual machines for further analysis.

From the analysis of the graph illustrated by Figure 6, it can be seen that the average CPU utilization in this experiment remained more constant than that of the previous experiment. This is due to the fact that there were more resources, that is, more virtual machines for the distribution of workloads. By relating the CPU Average graph to the Resource Utilization graph, it can be noted that when the CPU reaches an average usage of approximately 80% the load balancer starts to allocate more resources. When the CPU Utilization Average reaches

100%, all resources are allocated to assist in processing the excess load, which includes the allocation of the public cloud machine.

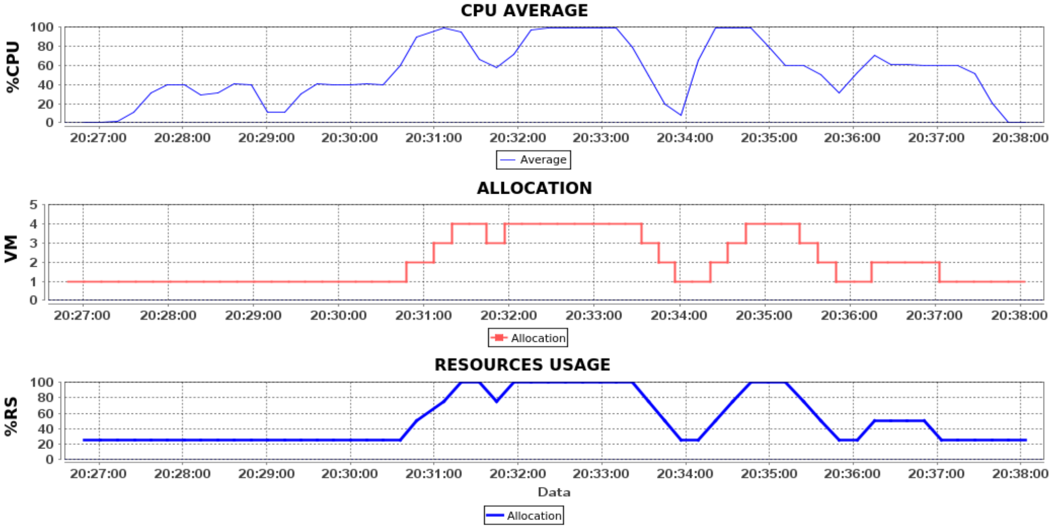


Figure 6: Experiment 2: Three virtual machine in the private cloud and one virtual machine in the public cloud. CPU Average Usage, Virtual Machine Allocation and Resource Utilization graphics

5 Final Remarks

Managing resource utilization in CC environments is an essential task. With the emergence of new technologies such as SDN and NFV, and their integrations with CC, this management becomes even more important. Therefore, the need for metrics that assess the quality of service of such environments is real. In the two presented experiments, the Resource Utilization metric shown results that match what was expected of the resource utilization of the analyzed environment. With the aid of the Average CPU metric it was possible to note that whenever the clouds were overloaded, more resources were allocated (virtual machines), which were available in the environment and the resources were being deallocated according to the load reduction.

In an integrated CC, SDN, and NFV environment, there is likely to be a need for resource allocation and deallocation (scaling up and scaling down)). However, the Resource Utilization metric would identify this allocation, but could have different behavior than it did in the experiments performed on the testing environment. This is future work to be planned and executed. Other intended future work is to design new metrics for quality evaluation for integrated environments, and to perform new experiments. Also, to use and scaling containers instead only virtual machines.

6 Acknowledgments

This work was partially supported by Universal MCTI/CNPq 01/2016 program (process 422342/2016-5).

References

[1] Siamak Azodolmolky, Philipp Wieder, and Ramin Yahyapour. Sdn-based cloud computing networking. In *Transparent Optical Networks (ICTON), 2013 15th International Conference on*, pages 1–4. IEEE, 2013.

[2] Laxmana Rao Battula. Network security function virtualization (nsfv) towards cloud computing with nfv over openflow infrastructure: Challenges and novel approaches. In *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*, pages 1622–1628. IEEE, 2014.

[3] Emanuel Coutinho, Danielo G. Gomes, and Jos De Souza. A tool for resource monitoring in computational clouds. In *8th Latin American Network Operations and Management Symposium (LANOMS 2015) - Application Session*, Joo Pessoa, Brasil, oct 2015.

[4] Emanuel F. Coutinho, Paulo A. L. Rego, Danielo G. Gomes, and José Neuman de Souza. An architecture for providing elasticity based on autonomic computing concepts. In *Proceedings of the 31st Annual ACM Symposium on Applied Computing*, SAC '16, pages 412–419, New York, NY, USA, 2016. ACM.

[5] Emanuel F. Coutinho, Paulo A. L. Rego, Danielo G. Gomes, and Jos N. de Souza. Physics and microeconomics-based metrics for evaluating cloud computing elasticity. *Journal of Network and Computer Applications*, 63:159 – 172, 2016.

[6] Emanuel Ferreira Coutinho. *FOLE: Um Framework Conceitual para Avaliao de Desempenho da Elasticidade em Ambientes de Computação em Nuvem.* Doutorado, Mestrado e Doutorado em Ciência da Computação (MDCC), Universidade Federal do Ceará (UFC), Fortaleza, 2014.

[7] Emanuel Ferreira Coutinho, Flávio Rubens de Carvalho Sousa, Paulo Antonio Leal Rego, Danielo Gonçalves Gomes, and José Neuman de Souza. Elasticity in cloud computing: a survey. *annals of telecommunications-annales des télécommunications*, 70(7-8):289–309, 2015.

[8] Nelma da Silva GOMES. **Qualidade de Software–uma necessidade**. *Especialista em Sistemas de Informação, com Pós-Graduação em Gestão Estratégica da Informação e Consultora da UCP/PNAFM/MF.*, 5, 2008.

[9] ISO/IEC. *ISO/IEC 9126-1*, volume 1. ISO/IEC, 2001.

[10] ISO/IEC. Iso/iec 25010: Systems and software engineering–systems and software quality requirements and evaluation (square)–system and software quality models. *International Organization for Standardization*, 34, 2011.

[11] Diego Kreutz, Fernando MV Ramos, Paulo Esteves Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky, and Steve Uhlig. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1):14–76, 2015.

[12] Jae Yoo Lee, Jung Woo Lee, Soo Dong Kim, et al. A quality model for evaluating software-as-a-service in cloud computing. In *Software Engineering Research, Management and Applications, 2009. SERA'09. 7th ACIS International Conference on*, pages 261–266. IEEE, 2009.

[13] Rashid Mijumbi, Joan Serrat, Juan-Luis Gorricho, Niels Bouten, Filip De Turck, and Raouf Boutaba. Network function virtualization: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, 18(1):236–262, 2016.

[14] Marc Oriol, Jordi Marco, and Xavier Franch. Quality models for web services: A systematic mapping. *Information and software technology*, 56(10):1167–1182, 2014.

[15] Balinder Singh. A systematic review on cloud computing. *International Journal of Engineering*, 2(2), 2013.

[16] Xianrong Zheng, Patrick Martin, Kathryn Brohman, and Li Da Xu. Cloudqual: a quality model for cloud services. *IEEE transactions on industrial informatics*, 10(2):1527–1536, 2014.

Short Papers

Towards a User Profile Generation Approach for IoT Applications

Cayk G. L. Barreto[*], Tales P. Nogueira, Marcio E. F. Maia, and Rossana M. C. Andrade[†]

Group of Computer Networks, Software Engineering and Systems
Federal University of Ceara, Fortaleza, Brazil
{caykbarreto, tales, marcio, rossana}@great.ufc.br

Abstract

Internet of Things (IoT) aims to connect everyday objects to the Internet, in which these objects communicate with each other and with people, thus, understanding both the environment and the users' needs. However, one of the main focuses of the academic research in this scope has been mostly the development of techniques for collecting, modeling, and reasoning about users' data to infer activities and to elaborate appropriate response strategies from the devices incorporated into the environment. On the other hand, this work focuses in the users' needs to propose an approach that performs modeling and contextual reasoning through user profiles, in which applications that use the approach can know the habits and preferences of a user from their profile and, then, perform actions in the environment that are more appropriate to the user.

1 Introduction

Internet of Things (IoT) is a paradigm that has been gaining a lot of attention in recent years. IoT is considered as part of the Internet of the future and will include billions of connected smart things (e.g. TVs). Studies show that by 2017 there were more than 8 billion IoT devices connected worldwide, with a market value estimated at over two trillion dollars, and by 2020 it is estimated that we will have more than 20 billion IoT devices connected to the Internet [1].

IoT promises to create a world where all objects around us are connected to the Internet and communicate with each other with minimal human intervention. The ultimate goal is to create "a better world for humans", where the objects around us know what we like, what we want and what we need, acting accordingly without explicit instructions [2]. One way to achieve this goal is through the construction of IoT applications, in which from sensors in the environment the system can understand the needs of the users and perform actions solving those needs.

There are several papers in the literature focused on recognizing users' needs and solving them in the scope of IoT [3, 4, 5]. However, there is an absence of works aimed at the development of approaches or techniques that identifies the knowledge generated from the sensors and build the user profiles, which can be used by applications to tailor its services to preferences and habits of the user in a given environment.

The objective of this paper is to present initial ideas towards the construction of an approach for the creation of user profiles in IoT environments, in which smart objects, from this profile, can perform actions in the environment where the user is. For example, in a smart home, when the application checks the user profile, it realizes that the user is usually watching TV at that

[*] This research was partially funded by INES 2.0, CNPq grant 465614/2014-0.

[†] Researcher Scholarship - Technological Development and Innovative Extension (DT2), sponsored by CNPq, Brazil

time, thus, the smart home application can ask if the user wants to watch TV and, if yes, automatically turn on the television.

2 Proposed Approach

This work aims to provide an approach for the generation of user profiles in IoT environments. Thus, applications that aim to work with contextual information from users can use the proposed approach to create profiles based on user habits and preferences in a given environment. Figure 1 shows the structure of our approach.

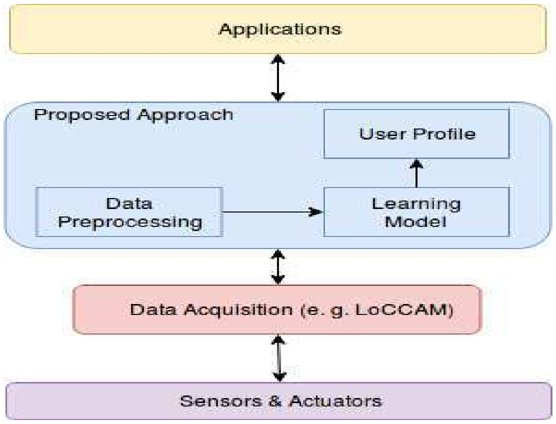


Figure 1: Proposed Approach

The idea is that the approach can be used by any type of IoT application or service. As shown in Figure 1, any kind of middleware such as LoCCAM [6] or FIWARE[1] can be used for data acquisition of the sensors as well as sending commands to actuators. User profile creation can be performed on both application servers and devices depending on the computational capacity of the available devices. Once the profile is created, applications can begin to act in the environment based on the information contained in the user profile.

For the application and testing of the proposed approach, it is necessary to have a set of data with activities performed by users in IoT environments. So, first, a literature review was realized in order to find open databases that contain the necessary information to create a user profile. The CASAS[2] Project was identified as a potential source of data as it contains several datasets with information about activities performed by residents in their homes [7].

A study about these datasets was then conducted to understand the types of data and whether these data could be used in the scope of this work. The following section presents a summary of the results found. To access all the results of the study the reader is referred to: `http://gitlab.great.ufc.br/cayk.l/Datasets`.

3 Preliminary Results: Datasets

The studied datasets were divided into four categories: i) three datasets in the city of Kyoto with information from two residents of one apartment; ii) two datasets in the city of Tulum

[1] https://www.fiware.org/

[2] http://casas.wsu.edu/

with data generated by a couple; iii) a dataset in the city of Aruba containing the information of one resident in his apartment; iv) a dataset containing the information of one person in his apartment. In the scope of this paper, we have brought only the analysis of the first three datasets.

3.1 Kyoto Smart Apartment - Two Resident Testbed

Three datasets with daily activities of two residents in the same residence on several different dates. The arrangement of sensors used to create the datasets is divided into two stages. The first one, without annotation, and the second one using annotation of the types of sensors. For this work, the schematic of the sensors with annotation was observed. The sensors were categorized into: M - motion sensor; I - item sensor for selected items in the kitchen; D - door sensor; AD1-A - burner sensor; AD1-B - hot water sensor; AD1-C - cold water sensor; T - temperature sensors; P001 - electricity usage.

For the latest dataset, the authors were able to identify 13 different activities through the used sensors, while in the other two datasets only 4 activities per user were mapped. The activities in common among all datasets were: the transition from bed to the bathroom, personal hygiene, sleeping, and working.

3.2 Tulum Smart Apartment - Two Resident Testbed

Two datasets with daily activities of a couple in their residence on different dates. In both datasets, the activities are annotated with markings showing the beginning and end of the activity. The sensors are categorized into two different types: i) M: motion Sensors; ii) T: temperature sensors. There is a variation in the number of sensors from one dataset to another. In the latest dataset (WSU Tulum Smart Apartment 2009-2010 Two Resident Testbed) there are 31 motion sensors and 5 temperature sensors, in the oldest dataset (WSU Tulum Smart Apartment 2009 Two Resident Testbed) there are 18 motion sensors and 2 temperature sensors.

In the most recent dataset (WSU Tulum Smart Apartment 2009-2010 Two Resident Testbed), the authors were able to identify 16 different activities, however, by checking the dataset, only 14 activities were found. On the other dataset, 10 activities per user were mapped, however, by checking the dataset, only 7 activities were found.

The activities “Leaving Home”, “Entering Home” and “Watching TV” is common to both datasets. In the first dataset, only the first activity (Leaving Home) is directly linked to a user, however, in the second dataset, only the last two activities are mapped to some user. The authors do not link the other activities to users, i.e., it is not possible to know who actually performed some activities. However, since some activities happen during a period that only one user was mentioned, we believe that these activities are related to that user.

3.3 Aruba Smart Apartment - One Resident Testbed

A dataset with daily activities of a woman at her home, which receives regular visits from her children and grandchildren. Activities are annotated with markings showing the start and end of each of them. The used dataset was the WSU Aruba Smart Apartment 2009 One Resident Testbed (Dataset 17). Sensors are categorized into three different types: i) M: motion sensors; ii) D: door sensors; and iii) T: temperature sensors. The authors were able to identify 11 different activities through the used sensors. In addition, they also inform how many times each activity was performed, for example, “Sleeping (401 times)”.

3.4 Analysis of the datasets

All the analyzed datasets have daily activities data of people in their residences. By observing the used sensors, it is possible to notice that motion and temperature sensors are used in all datasets. Other sensors, such as door sensor, appear in multiple datasets, however, it is not contained in all datasets.

Using the mentioned sensors, it is possible to know when a user enters and leaves the house, the movement of the user inside the house, in which moments he or she is in each room and for how long. Also, it is possible to know the temperature of the house. Regarding user activities, there are small variations from one dataset to another. For example, a dataset will not have the activity "Watching TV" while the others datasets will have the activity. However, there are 4 activities that are repeated in all datasets, namely: i) transition from the bed to the bathroom; ii) personal hygiene; iii) sleeping; and iv) work.

In the Kyoto and Tulum datasets, only a few activities are annotated with the user that have performed them. Therefore, it is impossible to determine which user performed some activities. The only dataset that does not have these problems is Aruba because there is only one user in the residence and the dataset is completely annotated with tags showing the beginning and the end of each activity. Therefore, we conclude that the best dataset to initially carrying out the tests of the proposed approach is the Aruba dataset.

4 Conclusion

This paper presented preliminar ideas of the proposal of an approach for creating user profiles in IoT, in which applications, services or middleware uses the approach to know the habits and preferences of the user in an environment and, thus, can take actions that help the user in that environment. The next steps of this work will be the preprocessing of the data obtained in the datasets studied; the application of the learning technique; and, finally, the execution of the experiments.

References

[1] Gartner, "Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016." https://www.gartner.com/newsroom/id/3598917, 2017.

[2] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on*, pp. 804–809, Ieee, 2010.

[3] A. M. Otebolaku and G. M. Lee, "Towards context classification and reasoning in iot," in *Telecommunications (ConTEL), 2017 14th International Conference on*, pp. 147–154, IEEE, 2017.

[4] A. I. Maarala, X. Su, and J. Riekki, "Semantic reasoning for context-aware internet of things applications," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 461–473, 2017.

[5] C. Tsirmpas, A. Anastasiou, P. Bountris, and D. Koutsouris, "A new method for profile generation in an internet of things environment: an application in ambient-assisted living," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 471–478, 2015.

[6] M. Maia, A. Fonteles, B. Neto, R. Gadelha, W. Viana, and R. Andrade, "Loccam-loosely coupled context acquisition middleware," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, pp. 534–541, ACM, 2013.

[7] D. J. Cook, "Learning setting-generalized activity models for smart spaces," *IEEE intelligent systems*, vol. 27, no. 1, pp. 32–38, 2012.

Indoor mmWaves Based Positioning System: Deployment and Evaluation

Lotfi Tamazirt[1*], Farid Alilat[1], Nazim Agoulmine[2]
[1] University of Sciences and Technology Houari Boumediene, Algiers, Algeria
[2] IBISC Lab, University of Evry Val-d'Essonne, Paris-Saclay University, France.
ltamazirt@usthb.dz, falilat@usthb.dz, nazim.agoulmine@univ-evry.fr.

Abstract

In our modern society, people spend a longer time in building (e.g. home, malls, etc.) or other closed areas (e.g. underground). GPS system is known to not perform well in these places while many context-aware services are requiring this information to provide the best service to them. In this paper, we address the problem of indoor positioning and particularly considering mm-waves that are emerging as the future communication spectrum. We aim to propose a novel three-dimensional (3-D) indoor positioning scheme. However, mm-waves have many issues to address such as exacerbation of path-loss, multipath propagation by the scattering, etc. In this paper we take into account Non-Line of Sight (NLOS) signals, Received Signal Strength (RSS) and Angle of Arrival (AoA) information to derive the most accurate position of the individual. We performed some simulations in order to highlight the relation between the accuracy of the localization that leads to the conclusion that the proposed positioning system yields a considerable accuracy improvement as well as the localization efficiency.

Keywords: Indoor Positioning System (IPS), Millimeter-Waves, Received Signal Strength, Angle of Arrival, Multipath, LOS, NLOS.

1 Introduction

Positioning in environment where satellite navigation is unavailable is a major challenge for people living in arid environments or where their positions is a critical issue. To overcome this situation, solutions such as WiFi, Bluetooth, RFID, UWB, NFC have been developed as a complement to GPS.

Unfortunately, with the exponential interest for applications and wireless services, the Radio Frequency (RF) spectrum is becoming very busy because of the multiplication of connected mobile devices (smartphones, tablets…). Therefore, considering the upper portions of the RF spectrum (i.e., Extremely High Frequency band) for wireless communications is a good solution since it is not used.

Millimeter waves (mmWaves) are the most likely candidates to be adopted by the 5th generation of communication networks (5G) [1], as they can achieve very high transmission with adoption of novel technologies for antennas that allow very dense spatial multiplexing. Although these advantages, strongly desired for 5G services (Smart cities, Biomedical services, Virtual Reality/ Augmented Reality and indoor localization), mmWaves brings also many technical challenges such as important Path Loss on high frequency carriers and the scattering.

Promising Indoor Positioning Systems (IPS) have been studied extensively in the literature as it is a critical component of many modern applications that require positioning information to provide their service however this location function is usually left to a third-party system. In this paper, we attend to study the design of an IPS based on mmWaves in a 3-D indoor environment. The objective is to investigate the level of accuracy that can be reached by such a system as well as the parameters that have the highest impact on this accuracy.

The rest of the paper is structured as follows. Section 2 describes a theorical overview on the localization algorithms. Section 3 presents the proposed localization analytical model. The model is implemented in a simulator and the performance evaluation results of the system are presented in Section 4. A discussion of these results is also presented in this section. Finally, Section 5 gives the conclusion of the paper.

2 Indoor localization algorithms

In many applications, multipath components are considered undesirable because they introduce errors in the estimation of the position especially NLOS multipath that deteriorates the accuracy [2]. In our work (following other state of the art work) [3-5], we believe that those components can be exploited as they carry spatial information. Moreover, as AoA technique outperform other methods in Line of Sight (LOS) scenario, it can be applied for those situations, and as RSS based positioning is not influenced by NLOS multipath as long as the path loss attenuation can be effectively evaluated and redressed, it can be used for LOS. Based on those facts, we are proposing a hybrid RSS/AoA technique in LOS and NLOS scenario.

Let consider $X_i = [x_i, y_i, z_i]^T$ with $i = 1, \dots, 4$, be the known coordinates for the ith transmitter, and $X = [x, y, z]^T$the coordinates of the Mobile Terminal (MT) that needs to be estimated. The estimated received signal strength $\widehat{P_{\iota RSS}}$ between the ith transmitter and the MT the can be expressed as follows:

$$\widehat{P_{\iota RSS}} = F_i \frac{P_i^t}{P_i^r} + \varepsilon_i \qquad (1) \qquad\qquad P_i^r = F_i \frac{P_i^t}{d_i^\alpha} \qquad (2)$$

Where F_i is an unknown deterministic parameter, $P_i^t$and $P_i^r$are the transmitted and the received power and ε_i a range of error. The received power can then be modeled as the equation 2. And where d_i is the distance between the transmitter and the receiver and α is the attenuation.

From the substitution of (2) into (1), we have:

$$\widehat{P_{\iota RSS}} = [(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2] + \varepsilon_i \quad (3)$$

Without considering ε_i, (3) can be expressed as:

$$\widehat{P_{\iota RSS}}^{2/\alpha} = x^2 + x_i{}^2 - 2xx_i + y^2 + y_i{}^2 - 2yy_i + z^2 + z_i{}^2 - 2zz_i \qquad (4)$$

In matrix notation, it can be expressed as:

$$G\Theta = H \qquad (5)$$

Where

$$G \triangleq \begin{bmatrix}\begin{bmatrix} x_1 & y_1 & z_1 & 0.5 \\ \vdots & \vdots & \vdots & \vdots \\ x_4 & y_4 & z_4 & 0.5 \end{bmatrix}\end{bmatrix} \; (6) \; \& \quad H \triangleq \begin{bmatrix} x_1{}^2 + y_1{}^2 + z_1{}^2 - \widehat{P_{\iota RSS}}^{2/\alpha} \\ \vdots \\ x_4{}^2 + y_4{}^2 + z_4{}^2 - \widehat{P_{4RSS}}^{2/\alpha} \end{bmatrix} (7) \; \& \quad \Theta \triangleq \begin{bmatrix} x \\ y \\ z \\ x^2 + y^2 + z^2 \end{bmatrix} (8)$$

After adding ε_i in (5), the minimization of the latest, the estimation of Θ is given by the least square solution as follows:

$$\widehat{\Theta_{RSS}} = arg \min_{\Theta} \big((G\Theta - \mathrm{H})^T (G\Theta - \mathrm{H})\big) = (G^T G)^{-1} G^T H \qquad (9)$$

Let us assume that (x_i, y_i, z_i) represent the coordinate of the position that comes out from the intersection of the spherical propagation of the waves emitted from transmitters.

The received signal can be mathematically expressed as:

$$\dot{y}(t) = \sum^{N_P} \sum_{\xi}^{4} \beta\,, \xi a^r(\widetilde{\phi^r}, \xi, \widetilde{\theta^r}\xi) + M_\xi(t) + \dot{n}(t) \quad (10) \text{ where } \quad M_\xi(t) = a^{tH}(\widetilde{\phi^r}, \xi, \widetilde{\theta^r}\xi) \,.\, \mathrm{x(t)} \qquad (11)$$

With Np is assumed to be the total sum of LOS and specular paths, $\phi^r \epsilon\ [0,2\pi]$ and $\theta^r \epsilon[0,\pi]$ being the azimuth and elevation of AoAs, respectively and $\xi\epsilon\{1,2,3,4\}$ represents the number of the reflection paths from the four surrounding walls.

3 System Modeling and Performance Evaluation

We considered in this paper a 3-D indoor scenario, with an assumed area of 30x30x3 meters. We suppose that 4 mmWaves Access Points (APs) are installed at appropriate positions on the walls. The positions are chosen such that it guarantees maximum coverage of any MT located in the room which position is unknown and needs to be estimated from the MT side. This later point is important as it differentiates with many other contributions which aim to estimate the position of the MT from the network side. Our system is configured with a Carrier frequency of 60GHz, a Transmission Power of 0.001Watts, a Transmission and Reception Gains of 1 dB respectively and 4 antenna arrays.

As mentioned before, angle-based positioning methods are more explicit about receiver position in LOS scenarios [6]. However, the MT can not know if the information received comes from a direct wave or generated by a reflection [5]. It is for this reason that in a second time, we will try to demystify from the different RSS indicators, the strongest signal according to the following assumption: The strongest received signal is necessarily the nearest emitted signal, knowing attenuation due to the phenomenon of reflection and multipath.

Hence, in what follows will present the performance of our mmWaves based 3-D indoor positioning system modeled on MATLAB R2017a. Indeed, Orthogonal Frequency Division Multiplexing (OFDM) technique has been adopted to provide orthogonality between signals emitted from each transmitter.

Figure 1 describes for its part a visualization of the cluster position from one of the four transmitter to the receiver. Each scattering cluster is approximated by 12 single reflections that has the same propagation delay. The spatial consistency model guarantees that path delays, angles and powers vary smoothly with time. It also highlights the LOS path, the First Bounce Scatter (FBS) and the Last Bounce Scatter (LBS).

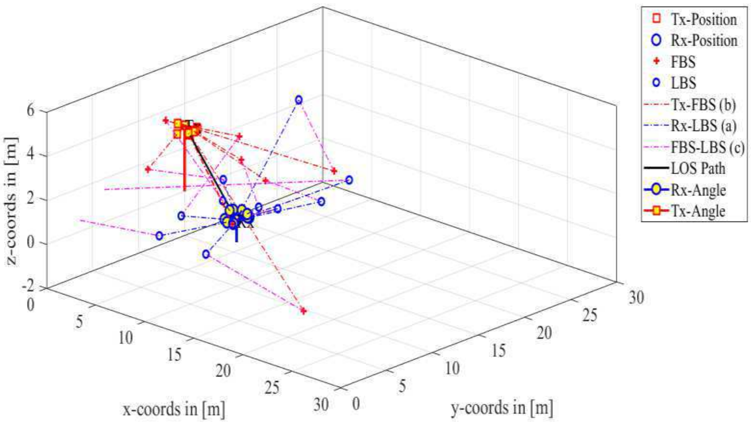


Figure 1: Visualization of cluster position.

For each path, the model derives the angle between the transmitter and the scattering cluster, the angle between the receiver and the scattering cluster and the overall path length which results in a delay of the signal. We plotted the collected data on the receiving device according to the proposed algorithm and we noticed that when the mmWaves encounters an obstacle, in our case, a wall, part of its energy is absorbed and a part continues to propagate attenuated after being reflected. Moreover, as the receiving antenna is only able to receive a small amount of the transmitted signal due to propagation in the air, we have assumed a threshold α for which the signal strengths lower than the latter are considered as NLOS and the higher or equal signals are considered as LOS. First results allowed us to see two distinct clusters, a first ranging from -108 to 134 dB, and a second spreading from -148 to -160 dB over 0.1 ms. This clear separation leads us to assume that the signals arriving in a reduced delay spread with a higher power are probably the signals that have not been reflected, and the signals that arrive with a lower power are those who have undergone reflections. However, after further study of possible cases, the assumption we made was proved insufficient, because a signal from a more distant AP can arrive with a lower power and in a larger delay spread (having traveled a greater distance) and that a reflected signal from an AP relatively closer to the receiver than the other APs, can arrive in a smaller delay spread, with a higher power. To overcome this issue, we proposed to introduce the distance component, in order to better distinguish the LOS signal from the NLOS signals.

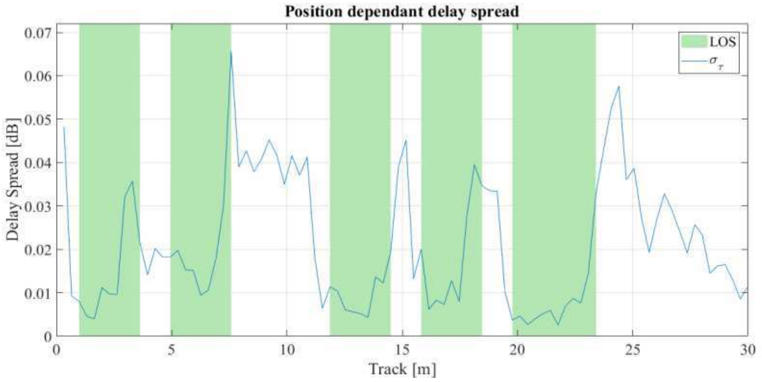


Figure 2: Position depending delay spread.

Figure 2 depicts the position depending delay spread on the room range. It shows the Root Mean Square (RMS) delay spread along the path. Shaded parts highlight the LOS segments. It also allows to notice that the delay spread gets shorter during LOS areas. An average estimation error of 43 cm was obtained through the use of this method for a MT positioned at $(10,10,1)^T$ versus an estimation of 72 cm without it which proves the efficiency of the approach. It slightly shows that the proposed method gives better performances for localization, however, a deeper study on the setup and the type of used antenna have to be addressed in future works to improve the localization accuracy and validated on a real test bench and thus validate the true value of the threshold α.

4 Conclusion

In this paper, a novel three-dimensional approach for indoor localization has been proposed. Experimental results indicate the effectiveness of the proposed method which exhibits a much better performance than without considering multipath components as well as determining if the received signal is a LOS or NLOS signal in order to improve the precision of the localization. However, such an approach has to be tested in a real scenario to be validated.

References

[1] Shahmansoori, A., Garcia, G. E., Destino, G., Seco-Granados, G., & Wymeersch, H. (2015, December). 5G position and orientation estimation through millimeter wave MIMO. In *Globecom Workshops (GC Wkshps), 2015 IEEE* (pp. 1-6). IEEE.

[2] Wielandt, S., & Strycker, L. D. (2017). Indoor multipath assisted angle of arrival localization. *Sensors*, *17*(11), 2522.

[3] Lemic, F., Martin, J., Yarp, C., Chan, D., Handziski, V., Brodersen, R., ... & Wawrzynek, J. (2016, September). Localization as a feature of mmWave communication. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2016 International* (pp. 1033-1038). IEEE.

[4] Vari, M., & Cassioli, D. (2014, June). mmWaves RSSI indoor network localization. In *Communications Workshops (ICC), 2014 IEEE International Conference on* (pp. 127-132). IEEE.

[5] Lin, Z., Lv, T., & Mathiopoulos, P. T. (2018). 3-D Indoor Positioning for Millimeter-Wave Massive MIMO Systems. *IEEE Transactions on Communications*, *66*(6).

[6] Tiwari, S., Wang, D., Fattouche, M., & Ghannouchi, F. (2012). A Hybrid RSS/TOA Method for 3D Positioning in an Indoor Environment. *ISRN Signal Processing*, *2012*.

Overview of NB-IoT communications in 5G

Donia DJEBALI[1], Nazim AGOULMINE[2], and Sonia BEN REJEB[3]

[1] Higher Institute of Computer Sciences of Tunis (ISI) Carthage University, Ariana, Tunisia and
IBISC Laboratory, University of Evry - Paris Saclay University, France
Donia_jebali@hotmail.fr

[2] IBISC Laboratory, University of Evry - Paris Saclay University, France
nazim.agoulmine@univ-evry.fr

[3] High School of Communication of Tunis (Supcom) Carthage University, Ariana, Tunisia
Sonia.benrejeb@supcom.tn

Abstract

Recently, two cellular technologies for Low Power Wide Area Network (LPWAN) have designed by the 3rd Generation Partnership Project to address the Internet of Things and the Machine to Machine markets. These are named Enhanced machine type communications (eMTC) or CAT-M1 and Narrowband internet of things (NB-IoT) or CAT-NB1. These technologies have been designed based on existing Long-Term Evolution (LTE) architecture with the objective of co-existance with existing LTE infrastructures, spectrum, and user equipements. However, there is a big difference between eMTC and NB-IoT not only in terms of targets applications but also of compatibility with LTE initial specifications. In the case of eMTC, a full compatibility was a requirement while for NB-IoT it was necessary to specify clean-slate specification to deal with the more constrained requirements in terms of scalability, coverage and energy consumption.

In this paper, we introduce the NB-IoT as presented in the 3GPP Release 13 in order to provide wide-area coverage, support a massive number of low-throughput devices and minimize the energy consumption and costs. We will also present an algorithm to evaluate the latency and the scalability in term of maximum supported number of devices.

1 Introduction

The market of the Internet of Things has experienced a mass deployment from 2 billion of connected objects in 2006 to 160 billion of them as 2018 [1].

These connected objects are already present in our daily life and some of them rely on cellular networks to communicate mainly GPRS or 3G. However, these technologies were not designed to support connected objects with important constraints in terms of energy consumption and coverage. Cellular technologies are therefore under important transition in order to support IoT communication more particularly with the 5G.

The 3rd Generation Partnership Project 3GPP, the group that has already standardized the 2G, 3G, 4G technologies has been working since several years on the 5th generation. In its release 13 of the LTE specification, it has released the first specifications of a 3GPP NB-IoT to address the needs of the IoT market and compete with other technologies such LoRa and SigFox. NB-IoT technology is considered as a very important technology and an important step towards the 5th generation of cellular networks. Industries, including Ericsson, Nokia and Huawei, have shown great interest in this new technology and have devoted a lot of efforts to contribute to its standardization. The objective of this paper is two folds. One is to introduce the NB-IoT technology. Secondly, the evaluation of the latency of the NB-IoT network, i.e the duration of all the steps from the time connected object initiate a connection to send data to a base station (eNodeB) until the time it received a confirmation of the transmission. In addition, we find it important to study the variation of this delay vs the possibly very large number of

connected objects deployed in the same cell.
The paper is organized as follows. After the introduction, a brief state of the art is exposed which highlight the various stage through a connected object passes when sending data. Then an algorithm is presented in the fourth section to evaluate the connected object communication as well as the adopted scenario to evaluate the important features of this technology. The final conclusion summarizes the work done and present future works.

2 3GPP NB-IoT system design

NB-IoT aims to offer deployment flexibility allowing an operator to introduce it using a small part of its available spectrum. It requires a minimum system bandwidth of 180 kHz for the downlink and the uplink. Choosing this minimum system bandwidth allows a number of deployment options [2]. In the downlink, the frame is structured in the time domain of 10 subframes of 1 ms. Each subframe is formed of two slots each one of 0.5 ms and each slot contains 7 OFDMA symbols. In the frequency domain, an NB-IoT carrier uses only one PRB LTE subdivided into 12 sub-carriers of 15 kHz for a total of 180 kHz [3]. NB-IoT provides a set of channels and physical signals that are primarily multiplexed over time which are mentioned in these articles [4][5].The NB-IoT uplink supports multi-tone and mono-tone transmissions. Multi-tone transmission is based on SC-FDMA like in the downlink. The mono-tone transmission supports 15 kHz and 3.75 kHz spacing. The numerology at 15 kHz is identical to the LTE. The 3.75 kHz Tone numerology uses a slot duration of 2 ms and can reach up to 48 sub-carriers [3]. In uplink, the NB-IoT includes also a set of channels and signals [4][5].

3 Data Transmission Phases

To transmit data, a NB-IoT UE needs to follow this specified phases. First, the device must obtain down synchronization which is an important step in cellular communications. When a UE is turned on for the first time, it must detect an appropriate cell, obtain for this cell the frame synchronization as well as the synchronization with the carrier frequency. Once the synchronization procedure is complete, it proceeds to the acquisition of the MIB. Then, it perform up synchronization during the random access period which is important to maintain the orthogonality of the uplink. The random access procedure consists of the exchange of four messages between the UE and the eNodeB. Once the random access procedure is complete, there is an additional exchange of RRC messages between the sensor and the eNodeB to establish the security and the quality of service for the connection. Finally the UE send its data. These phases are explained in details in [4].
In NB-IoT systems, each NPUSCH or NPDSCH transmission is preceded by associated control information transmitted via a NPDCCH. Depending on the reception of the control signals, the UE can establish the level of coverage and consequently the number of repetitions. In addition to the time of the downlink grant, there is an additional time which corresponds to the time of channel changes explained in [5].

4 Simulation and results

The environment consists of an LTE cell and a eNodeB. The cell is divided into three areas which differ according to their distances from the eNB. The sensors will be dispersed in an irregular way according to their coordinates (x, y) on the three areas.

4.1 Algorithm

Algorithm 1 Calcul latency (Data,TBS,NRB,RBU,per,n)

```
**Input:** Data length of data ,TBS length of Transport Block Size ,NRB number of ressource block ,RBU number of ressource block per user, per reporting period, n number of UEs, TLu time due to channel/liaison change, repetitions and time to sent DCI.
**Output:** Evolution of delay in function of the number of UEs.
$A[N][7] \leftarrow 0$
for $i = 1$, $i{+}{+}$, $i <= n$
$A(i,1) \leftarrow random([-500, 500])$ /* coordinate X of the sensor */
$A(i,2) \leftarrow random([-500, 500])$ /* coordinate Y of the sensor */
$A(i,3) \leftarrow sqrt(A(i,1)^2 + A(i,2)^2)$ /* Distance separating the sensor and the eNB */
$A(i,4) \leftarrow Pe * ((c/f)/(4 * pi * A(i,3)))^2$ /* Received power*/
**if** $A(i,3) <= d1$ /* d1 perimeter of area 1*/ **then**
    $A(i,5) \leftarrow 1$ /* sensor is in area 1 */
**else if** $(d1 < A(i,3))AND(A(i,3) < d2)$ /* d2 perimeter of area 2*/ **then**
    $A(i,5) \leftarrow 2$ /*sensor is in area 2 */
**else**
    $A(i,5) \leftarrow 3$ /* in area 3 */
**end if**
end for
/* Calcul of number of sensors per area */
for $j = 1$, $j{+}{+}$, $j <= n$
**if** $A(j,5) = 1$ **then**
    $Narea1 \leftarrow Narea1 + 1$
    $TLu1 \leftarrow T1$
**else if** $A(j,5) = 2$ **then**
    $Narea2 \leftarrow Narea2 + 1$
    $TLu2 \leftarrow T2$
**else**
    $Narea3 \leftarrow Narea3 + 1$
    $TLu3 \leftarrow T3$
**end if**
end for
$Narea \leftarrow [Narea1, Narea2, Narea3]$
$TLu \leftarrow [TLu1, TLu2, TLu3]$
for $m = 1$, $m{+}{+}$, $m <= 3$
$Delay(m) \leftarrow TLu(m) * (Data/TBS(m))$ /*Delay for one UE*/
$Nmax(m) \leftarrow (per/Delay(m)) * (NRB(m)/RBU)$ /* Maximum number of UE by report period */
for $k = 1$, $k{+}{+}$, $k <= Narea(m)$
$D \leftarrow Delay(m) * (k/(NRB(m)/RBU))$
tracer curve(k,D) /* Evolution of delay in function of number of UE */
end for
end for
```

4.2 Adopted scenario

To evaluate the performance of the NB-IoT system, we developed a simulator using MATLAB environment. This simulator models the main characteristics of this technology, the number of repetitions, the time of link and channel changes, etc.
We observe that more the number of UEs increases, more latency per user increases. This occurs because as the number of UEs increases, the probability of waking up and finding available uplink resources decreases (due to resource limitations since the NB-IoT uses only one LTE PRB). We can also note that the latency is much weaker if we move away from center. This can be explained by the fact that moving away from the eNB the signal quality is degraded and to guarantee the good reception of the latter, it is sent several times (the number of repetitions used increases to satisfy the UEs located at the edge of the cell) and the TBS decreases. And if the number of users exceeds the support capacity of the area, we can notice that the time diverges to extremely high values. eNB, which has only one PRB, can no longer guarantee delivery of UE reports in a timely manner. this explains that the demand of some UE is rejected.

5 Conclusion and future works

This article consists of two main parts, in the first part we study a recent LPWAN technology namely NB-IoT, based on LTE. In the second part we evaluate the performances of this new technology: The latency and the scalability. We show that these metrics depend on MCL, TBS, channel bandwidth, data length, RF switching delay, subframe delay, and reporting period. In addition, we present a network simulation tool that can evaluate these two NB-IoT performance metrics in an environment that we specify in this document.
Now we want to highlight some interesting extensions of our project. We can adapt the realized simulator to evaluate the latency as well as the scale transition of the eMTC, the IoT technology also developed by the 3GPP during version 13. We can study the performance of these two IoT technologies against other performance criteria such as power consumption or battery life.

References

[1] Lothar Walther, "Internet of Things - IoT System Design Challenges and Testing Solutions", Training Center Rohde Schwarz, white paper, 2017.

[2] Yihenew Dagne Beyene, Riku Jntti, Olav Tirkkonen, Kalle Ruttik, Sassan Iraji, Anna Larmo, Tuomas Tirronen, Johan Torsner, "NB-IoT Technology Overview and Experience from Cloud-RAN Implementation", IEEE Wireless Communications, Vol 24, pp 26 - 32, June 2017, DOI: 10.1109/MWC.2017.1600418

[3] 3GPP TS 36.211, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation (Release 13), 2018.

[4] Y.-P. Eric Wang, Xingqin Lin, Ansuman Adhikary, Asbjrn Grvlen, Yutao Sui, Yufei Blankenship, Johan Bergman, Hazhir S. Razaghi, "A Primer on 3GPP Narrowband Internet of Things (NB-IoT)", IEEE Communications Magazine, Vol 55, pp 117 - 123, March 2017, DOI: 10.1109/MCOM.2017.1600510CM.

[5] Rapeepat Ratasuk, Nitin Mangalvedhe, Yanji Zhang, Michel Robert, Jussi-Pekka Koskinen, "Overview of Narrowband IoT in LTE Rel-13", 2016 IEEE Conference on Standards for Communications and Networking (CSCN), Oct/Nov 2016, DOI: 10.1109/CSCN.2016.7785170

Service Execution Orchestrator for IoT

Lucas Sales Vieira, Marcio E. F. Maia, and Miguel Franklin de Castro

Group of Computer Networks, Software Engineering and Systems
Federal University of Ceara, Fortaleza, Brazil
lucasvieira, marcio, miguel@great.ufc.br

Abstract

The number of devices connected to the Internet already surpasses the human population causing the Internet of Things (IoT) to grow. The Internet of Things uses the concept of everyday objects endowed with sensors and actuators, communicating in order to provide services. In this context, it is possible to cite some scenarios such as houses, buildings and intelligent hospitals in which diverse sensors and actuators help in the routine of every day's, these sensors and actuators most of the times are executed in runtime. For this scenario to work efficiently it is necessary to use a technology that supports data overload such as cloud computing and orchestrators. However, when applied to the Internet of Things, these concepts need to be revised, since the quantity, dynamicity, and heterogeneity of the interacting devices introduce new challenges. Thus, this work proposes a fault-tolerant orchestrator for IoT application, in order to reduce the throughput data overhead generated by IoT applications in addition to being able to state previous faults so that they can be executed again.

1 Introduction

The Internet of Things (IoT) has been highlighting, both in industry and academy, because of its central idea that everyday objects or things are connected to the Internet, exchanging information to achieve certain goals and interaction with users. This scenario also has the premise that such objects, through learning techniques, can infer users' wishes and adapt services [12].In 2003, the proportion of the number of devices connected to the Internet was around 500 million to about 6.3 billion people, and even though it seems distant, it is estimated that in 2020 this number will reach 24 billion [9].

The heterogeneity of devices, systems, and services is latent in such a scenario. For example, a service support technology, we can mention Cloud Computing. In the Cloud Computing scenario, it is possible to promote service scalability [11]. However, the IoT scenario is dynamic and devices are not always available, and the use of services may be higher or lower, requiring more of the cloud resources. Therefore, server elasticity is an important requirement for optimizing resources in this context.

Therefore, design-time decisions make rigid adaptations at runtime. As an alternative, the use of self-adaptive systems concepts shows a possible solution to the flexibility of the IoT scenario. Furthermore, it is a self-adaptive system (SAS) that is capable of being modified and its attributes or artifacts in response to internal or external changes [8].

Based on what has been discussed in the previous paragraphs, the goal of this work is to develop a fault tolerant orchestrator for the Internet of Things. IoT services will be run on containers that will be deployed on devices that have been in the fog, the orchestrator will be responsible for managing and making decisions regarding device management. The rest of the paper is divided as follows: in section 2 the background; section 3 related works; section 4 Proposed Approach; and, finally, section 7 conclusion.

2 Background

2.1 Internet of Things

The term Internet of Things (IoT) was first used by Kevin Ashton in 1999, and over the years gained strength and space in different areas such as e-health, smart homes, and buildings, or traffic [4]. In the last years, IoT has been growing day after day, and the idea of objects that can exchange information and act on the user context has been growing at the same pace. These objects are called intelligent objects and are endowed with the ability to detect and act on the environment in which they are inserted, as well as the ability to exchange information between them [11].

Impacts can occur due to the advancement of the IoT paradigm, since the objects referred to perform actions that directly affect our daily lives through the emergence of applications for the various areas of IoT performance, such as smart homes, buildings and everyday learning, among others [4]. Therefore, there are several contexts in which IoT can act and create new applications to act indirectly or directly in our lives.

Thus, IoT allows the creation of new services and new approaches to existing services [10].In IoT, objects learn from user activities, thus creating intelligent objects. In this context, an example of an intelligent object is Mother Sense, a system for monitoring physical objects, being able to provide details about the activities of monitored objects, as well as send notifications, reminders, and alerts [14].

3 Related Work

In this section will be presented works related. In the first work [5], the authors developed an orchestrator based on the platform called LiquidIoT that allows the deployment and management of IoT devices. The orchestration created is divided into three parts set of participating applications, variables used for runtime data staging, and actions that define orchestration streaming. To perform the orchestration first, the application discovers all the intelligent objects, then verifies which of these are of interest of the user then performs a query to find out which of these it is possible to monitor and then realizes the deploy of the application, sending and receiving data is done using JSON.

In [6], it focuses on a fault-tolerant framework for IoT systems that can preserve its previous state of failures, thereby causing the system to continue performing its intended actions. In order to perform these structures, the data will be judged based on different parameters in the local cluster and the cloud platform and the other motivation of the authors is to adopt computing resources from the edge to the side of the cloud. In this way services can be managed at the edge of the network minimizing the physical distance delay, consuming less bandwidth and providing flexibility in the choice of the processing location.

One of the major forms of fault tolerance is through replication on edge devices, to achieve a decrease in processing time some data is processed in edge devices, thus decreasing response time, provides means to run applications on both the devices edge and in the cloud without requiring source code changes and provides application portability and management. As we can see, none of the studies performed to try to improve the decrease in the data transfer rate and fault tolerance together, is this the main differential of the proposed work.

4 Proposed Approach

This work proposes a service orchestrator for IoT that is fault tolerant and manages the devices related to the context in which the user is. The definition of the context used to perform this work will be [15] that we can consider an extension of the definition of [3]. For [3] the context definition is any information that can be used to characterize the situation of an entity, where that entity can be a human being, an object that is relevant to the interaction between the user and the application, this includes the user and the application, in [15] we have an extension in the definition, since we removed the limitation of the interaction of the application with the user and context becomes information that can describe situations of the entities involved in a relationship that is important for the app.

In addition to what has been mentioned previously, this work will be an advance of [1] and [7]. The work of [1] allows the discovery of intelligent objects and control them by means of context sensitivity, having as an important contribution the decrease of the data transfer rate and the work of [7] was to create a framework called Support Mechanism for Creating and Executing workflows for Decoupled SAS in IoT (SUCCEEd) in which the main contribution was an orchestrator that allows the execution of adaptations that is able to select, at runtime, the most suitable adaptations for a given system state or context.

This work takes a step forward from the two previously mentioned because it will use the [1] context discovery using an orchestration approach similar to that discussed by [7], in which it used the MAPE-K loop which is a control loop for the self-adaptation process and through this model it is possible to monitor, analyze, coordinate and evolve at runtime [2]. To create the orchestrator it will decrease the amount of messages exchanges and help in fault tolerance.

Then, to create the orchestration, we will use the MAPE-K loop where we will use each phase of the loop that are: Monitor (M) is the layer that receives the data, which in turn are filtered and characterized until some action is necessary and then it is sent to the Analysis layer (A); in this phase the desired state will be analyzed with the known one and in case it is necessary to make some change then the Plan phase (P) will be executed, in that phase it will be realized how the change will occur in the system to be executed in the execution phase (E). Finally, there is the Knowledge (K) phase that consists of a grouping that state, objectives, policy, requirements, actions, and characteristics of the system and this information is executed whenever the MAPE-K Loop is executed.

To create the fault tolerance part of the proposed approach will be used RabbitMQ. RabbitMQ is an open source software that allows it to be implemented to support the protocol called Advanced Message Queuing Protocol (AMQP). Through it, it is possible to create applications that handle the exchange of messages that are in the system [13]. Therefore, we will use these technologies to support the execution of the data sent and thus guarantee the fault tolerance of the orchestrator. RabbitMQ would be in the running part of MAPE-K Loop and every lifetime an action would execute would wait for the success or failure response to have the action executed again or not. Finally, the reduction of the message exchange rate is accomplished through CoaP-CTX, because in the experiments performed by [1] it is possible to verify that there is a significant reduction in the number of message exchanges exchanged between objects and application, thus guaranteeing one of the differentials of the work of this article.

5 Conclusion

This article presents a contribution to the development of an approach for the orchestration of services in IoT, in which it presents as differential the decreased throughput of data in the network together with the fault tolerance. The next steps of this work will be the development of the orchestrator based on the MAPE-K loop and the integration with the CoAP-CTX and finally will be realized experiments for the validation of the approach.

References

[1] Felipe M Barreto, Paulo A de S Duarte, Marcio EF Maia, Rossana M de C Andrade, and Windson Viana. Coap-ctx: A context-aware coap extension for smart objects discovery in internet of things. In *Computer Software and Applications Conference (COMPSAC), 2017 IEEE 41st Annual*, volume 1, pages 575–584. IEEE, 2017.

[2] Autonomic Computing et al. An architectural blueprint for autonomic computing. *IBM White Paper*, 31:1–6, 2006.

[3] Anind K Dey, Gregory D Abowd, and Daniel Salber. A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications. *Human–Computer Interaction*, 16(2-4):97–166, 2001.

[4] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7):1645–1660, 2013.

[5] Otto Hylli, Anna Ruokonen, Niko Mäkitalo, and Kari Systä. Orchestrating the internet of things dynamically. In *Proceedings of the 1st International Workshop on Mashups of Things and APIs*, page 4. ACM, 2016.

[6] Asad Javed et al. Container-based iot sensor node on raspberry pi and the kubernetes cluster framework. 2016.

[7] Belmondo Rodrigues Aragao Junior, Rossana Maria de Castro Andrade, Marcio Espindola Freire Maia, and Tales Paiva Nogueira. Succeed: Support mechanism for creating and executing workflows for decoupled sas in iot. In *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, pages 738–743. IEEE, 2018.

[8] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. Future internet: the internet of things architecture, possible applications and key challenges. In *Frontiers of Information Technology (FIT), 2012 10th International Conference on*, pages 257–260. IEEE, 2012.

[9] Alan Tomás Lima. *Aplicação de Internet of Things em casas inteligentes-Serviço Aplicacional.* PhD thesis, Instituto Politécnico do Porto. Instituto Superior de Engenharia do Porto., 2014.

[10] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497–1516, 2012.

[11] Francesc D Muñoz-Escoí and José M Bernabéu-Aubán. A survey on elasticity management in paas systems. *Computing*, 99(7):617–656, 2017.

[12] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. Context aware computing for the internet of things: A survey. *IEEE communications surveys & tutorials*, 16(1):414–454, 2014.

[13] RabbitMQ. Rabbitmq - rabbitmq is the most widely deployed open source message broker. disponvel em https://www.rabbitmq.com. ltimo acesso em novembro de 2018. 2018.

[14] Mother Sen.se. **Mother Sen.se**. disponvel em https://sen.se/mother/. ltimo acesso em novembro de 2018. 2018.

[15] Windson Viana, Alina Dia Miron, Bogdan Moisuc, Jérôme Gensel, Marlène Villanova-Oliver, and Hervé Martin. Towards the semantic and context-aware management of mobile multimedia.

Multimedia Tools and Applications, 53(2):391–429, 2011.

Efficient management of residues collection
Study case – Praia City

Alexsandro Baptista, Carlos Correia, Helder Gomes And Ivanildo Silva
University of Cape Verde

Abstract

Residues are one of the major problems that all cities around the world are facing nowadays and Praia is not an exception, therefore, it suffers from several problems derivative of residues. For example, high cost in residues collection management, accumulation and disorganization of residues in containers, roadways, neighborhoods, and some other undesirable places, and containers invasion of people and animals bringing innumerous constraint and negative impacts on health, environment and most of all in economy. According to the Atlas report of the renewable energy in Cape Verde, Santiago Island produces about 220 tons of trashes daily, where about 70% of that amount is centered in Praia city, a number that is growing day by day. [1] The city hall of Praia (CHP), entity responsible for the management of the county residues has the budget in 2018 of 90 thousand Cape Verdean Escudos (CPE), for the global cost of the residues management, the most expensive parcel correspond to the collection and transportation of the residues, this can represent between 40% to 70% of total management costs. [2] [3] It is extremely urgent to think about adopting a more efficient management of the residues collection in which can help to rectify the constraint of the residues in the county. In this sense, the project Efficient Management of the Residues Collection (EMRC), permits to automatize the residues containers, residues collection vehicles to optimize the routes of the residues collection.

Keywords: Automation, optimization end geo-referencing.

1- Introduction

Having into consideration problems due to residues in Praia city, which have impact in health, environment and economy, this project was chosen based on three essentials motivating aspects: High cost on residues management, disorganized accumulation of several types of residues (organic and non-organic). Walking around some neighborhoods streets in Praia it is frequent to find piled trashes in the open sky, becoming very uncomfortable for any citizen to pass by, without saying that, these piled trashes serve as nests for insects and other homeless animals and invasion of the containers that people and animals do, facilitate the propagation of virus and diseases like dengue and malaria.

Objectives

The project is based on three major objectives:

- ✓ To reduce the cost of the management of residues collection in Praia;
- ✓ To contribute to a clean city;
- ✓ To preclude the invasion in the containers;

2- Project Description

EMRC is a computational system based in automation, computerization and geo-referencing of the containers and residues collection vehicle, permitting monitoring the levels of the residues in the containers and residues collection vehicle remotely and in real time. Each one of the container (slave) possesses sensors that can read the level of the residues and send it to the central (master) through a message, in which, collects these data of several different containers and send it to a server through a serial and it stores them on the database. With the data levels of the residues of the different containers in different neighborhoods, the system traces its own route of collection based on the full containers, distance between them and the car traffic, optimizing residues collection. Beside system allows to geo-referencing the containers and residues collection vehicle, also permitting to manage reports and exhibiting alerts to population when the collection vehicles are approaching in door-to-door pick-ups.

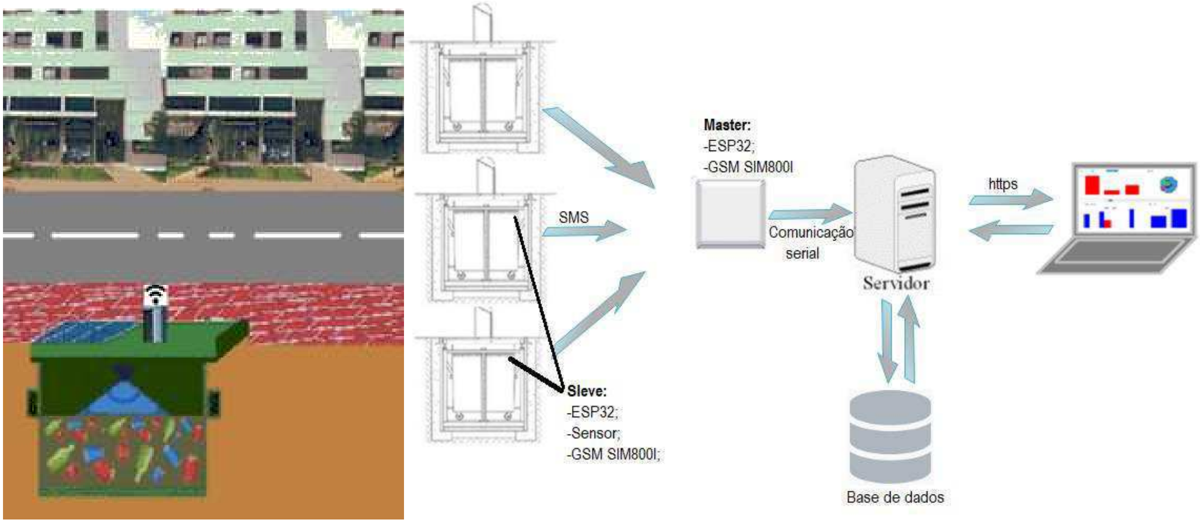


Figure 1 – description of the project operation

Residues Containers Automation

Containers automation are built of radar level sensor RCWL-0516 that read the residues levels, micro-controllers ESP32 that read sensor information, GSM SIM808 which sends data of the levels of the collected residues by the micro-controller and the geographic localization of the master container. In each collection residues vehicle contains a micro-controller ESP32 and a GSM SIM808 that sends to the server geographic points of the vehicle in real time through HTTP.

Computerization and Geo-referencing

The system is prepared to trace its own route based on full containers, distance between them and roads traffic, in this case, optimizing the route of the residues collection. It also alert about the changes of containers positions in case of theft and vandalism of the same. The system allows to geo-referencing all containers in an interface with the level of residues of each containers in a real time, it also monitor the collection residues vehicles in real time, timing each collection to a possible forecast and report preparation.

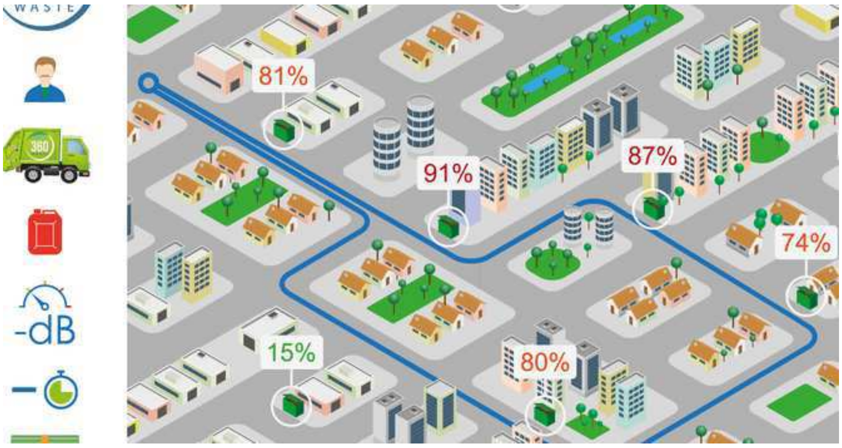


Figure 2 – Containers Geo-referencing page. Source: [4]

System consumptions and powering System

Automation systems that are installed in the containers, *the master* installed in the server and also those installed in collection vehicles have a consumption of approximately 11wh when the data are transferred. Each one of the containers are equipped with an autonomous powering system made of a solar panel of 10wp, 12v, a rechargeable battery of 12v, 20Ah. *The Master* and the modules that are in the collection residues vehicles are powered directly by the USB cable, which connects to the server for data traffic through serial.

Project Costs and benefits

The project costs around 3 332 500 CVE to a kit of 200 containers and 10 automatized collection vehicles, equivalent to a 15 900 CVE for each automatized container. The project cost tends to diminish as much as the numbers of these containers and automatized collection vehicles increases. From the test made in the Barreiro neighborhood, Portugal, by Ana Filipa Pereira Beijoco, in her Master□s dissertation, it was optimized by time and distance appealing tools of geographic information system ESRI ArcGIS about them calculated the results of the travelling time, distance, pollutants emissions having into consideration, the influence of dynamic transport of cargo, gas consumption and costs. By optimizing the route, it allowed savings of 57% of the residues management costs. The reduction on the average values of pollutants emissions vary between 40% to 50%, depending on the compound, and the average time diminish about 62%. [2]

It contributes to a clean city, the residues will be organized because of the collection on time and well-guarded in a way that precludes the invasions of this containers. Decreasing of the negatives impacts on health and environment of the disorganized and accumulated residues will be crucial.

Bibliographic

[1] C. D. M. BO, “Atlas Energias Renóvaveis,” Registo legal, nº 2/2001, Feverreiro de 2012.

[2] A. F. P. Beijoco, “Optimização de um Sistema de Recolha e Transporte de Resíduos Sólidos Urbanos,” Instituto Politécnico da Universidade Tecnica de Lisboa, Portugal, Maio de 201.

[3] N. M. R. Martins, “ANÁLISE E OPTIMIZAÇÃO DA RECOLHA DE RESÍDUOS: CONTRIBUTOS DE UM SIG PARA A ÁREA DE GESTÃO ASSEGURADA PELA CMPORTO,” Instituto Politécnico de Viana de Castelo, Fevereiro de 2015.

[4] A. Sousa, “360Waste: um sistema de gestão inteligente de resíduos,” 20 Fevereiro 2018. [Online]. Available: https://www.techemportugues.com/2018/02/20/360waste-evox-technologies/. [Acedido em 20 Julho 2018].

Future Internet: **TALKING WITH 5G**

Janet da Luz & Nilza Rocha
Computer Systems Engineers
Telco Workers

Abstract

We are facing new communication and networking challenges. With 5G countries and organizations are trying to provide better, more sophisticated, smarter and faster technology.
This is a preview of what is 5G, its benefits and challenges and how Cape Verde could gain from such technology evolution.

Introduction

There are many challenges in this 21st century.
One of them is to think about how wireless network and the internet evolution can impact our lives.
We have been witnessing several changes in the way people seek and manage its preferences among a multiplicities of technologies alternatives around us.
Going straight to the point, our evolution is being paced by technological evolution, as mobile evolve from the analog in 1G to fully digital in 5G, introducing IoT infrastructure ecossystem.

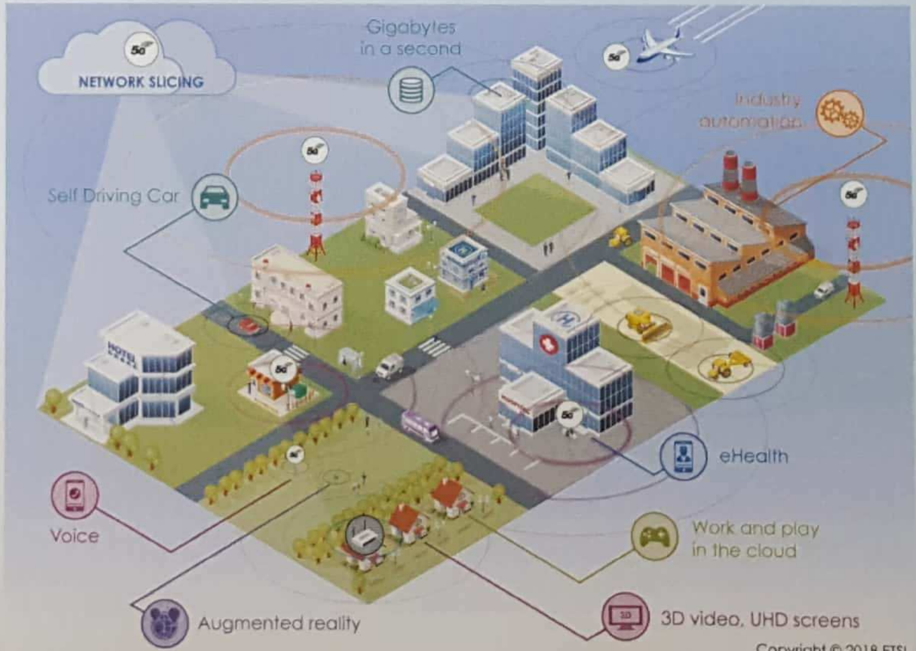
What is 5G?

But what is this so called 5G? Where did it come from?
As described in IEEE Standards Association 5G is the fifth generation of mobile communication. It is based on wireless communication and it aims to increase data speed.
"5G is not just about faster, bigger or better. It's about enabling a diverse new set of services and use cases affecting nearly every aspect of our lives. But to live up to their potential, 5G-enabled applications must be delivered securely."
"The history of 5G is being made…now. It is being born into a competitive world where mobile network operators, system vendors and regulators will shape what eventually emerges. If all goes well new 5G systems could begin to be rolled out from around 2020 (nearly 30 years after the first GSM systems were rolled out). 5G is a global initiative that will play out in different ways in different countries…"
A formal 5G pattern has not yet been defined, according to the Next Generation Mobile Network's 5G white paper, 5G connections must be based on 'user experience, system performance, enhanced services, business models and management & operations'.
5G is tipped to be the mobile network for the internet of things and big data.

Why do we need 5G?

Many benefits are associated with this generation.
Data volume is increasing because customers are using more connections to quickly access a range of services. With 5G we can ensure the maximum operational performance to prevent high levels of energy consumption, equipment and operational costs and network development.
Cost reduction (capital), productivity, efficiency, quality of service, cloud services, cloud Telco with wireless network connection, simple access, relevant and personalized content are other benefits from 5G.
None of this is possible if there is no required technology and infrastructure capable of supporting all these services.
Sometimes it can be the number one issue: solving the problem between infrastructure and services management.

5G is associated to a large variety of sectors. There common point will be the technology used to provide services to sectors like industry, education, transportation, healthcare, retail, energy, media and networking.
This generation has its own challenges. To understand it we can think about questions like "Will 5G be viable?", "Will it be the technology supported by developed countries or developing countries will take benefits from it?". Because it is mandatory to invest in research, technology processes and infrastructure.
Beside technology challenges like traffic management, access control, machines and terminals there are also other challenges like legislation, multiple services, standardization and application of 5G services, communication, navigation, privacy and security.



Copyright © 2018 ETSI

Is it useful in Cape Verde?

Cape Verde is a developing country facing new opportunities and challenges and trying to enlarge communication and integration between sectors.
Evolution to 5G will allow the development of concepts and services for smart cities, safe cities, education, parking zones, surveillance and healthcare given that these sectors can be upgrated with networking, services integration, access control and remote connection.
Cape Verde has maintained fundamental conditions for economic development namely, security and stability, building solid institutions (and striving to continuously improve them).
Currently, Cape Verde is using 2G (GSM 900, GSM 1800) and 3G (UMTS 2100).
But with 5G upgrade Cape Verde can solve many issues, particularly in the healthcare sector.
Healthcare is a challenge to any archipelago.
The transport of patients to the main hospitals (due to the lack of adequate equipment at all healthcare posts) has caused many inconveniences in Cape Verde. Other situation is related to the giant waiting time in emergency services.

Use case categories in healthcare

"Wearable devices, secure online consultations, and remote procedures like robotic surgery will improve resource efficiency and meet consumer demands for greater convenience and freedom of choice."

Conclusion

5G can provide significant improvements to our daily routines.
It will satisfy a multiplicity of requirements and developing countries - especially African ones - should pay attention to development enablers and make continuous efforts to growth and gain sustainability.
Cape Verde can take advantage of these efforts to increase the conditions of service provision. Instantly, healthcare is one of the areas where these services can be significantly improved: for example, using telemedicine as a way to offer remote assistance.
Meanwhile it is still possible to use this fifth generation to explore and upgrade other sectors.

KA TEN DOKUMENTU – An exploratory empirical research on students generated content : the case of Communication and Multimedia students of the University of Cape Verde on criolo identity

Álvaro Patricio Elgueta Ruiz
University of Cape Verde
alvaro.ruiz@docente.unicv.edu.cv

José Augusto Abreu Fernandes
University of Cape Verde
jose.abreu@docente.unicv.edu.cv

Abstract

The present work seeks to present an exploratory case study of transmedia narratives in a formal university academic context in an African archipelago country (Cape Verde). The methodology of the work was the one of research-based in the scope of the discipline of Cyberculture, made with students of the third year of course of Communication and Multimedia. The narrative master line has been the expanded understanding of the legal status of the human person promoting non-discrimination based on this status. They worked with « *life stories* », using various digital platforms from undocumented Cape Verdean migrants living outside Cape Verde. Among its main results is the ease of use of certain platforms over other (mainly Facebook), as well as the diversity of narrative contents presented by the students. It is concluded that the transmedia narratives are efficient tools for the use of teaching-learning in complex contexts of migration, multiculturalism, and multilingualism.

Keywords: Transmedia Narratives, Migration, Multilingualism, Higher Education, Digital Anthropology, Ethnography.

1 - Introduction

Cape Verde is a small insular country on the west coast of Africa with 500,000 inhabitants divided by 10 islands (Praia, the capital, has 140,000 inhabitants) and with an equal number living in the diaspora (mainly in Portugal, the Netherlands and the United States). Old portuguese colony with different status from that of the other Portuguese colonies in Africa, Cape Verde has as its native language the Creole (without a stabilized written tradition) and Portuguese is the official language (as well as the language of inheritance). Martirized by long periods of drought, many Cape Verdeans find in emigration a form of survival. The privileged relations with Portugal have allowed a register of tolerance with generations of emigrants arriving in Portugal without formal conditions to be welcomed. Existing kinship networks coupled with an affective proximity between Portuguese and Cape Verdean allowed a first generation of emigrants conditions of survival to people without any kind of legal framework as emigrants. The inclusion of the descendants in the Portuguese administrative environment has created great problems of documentary legality running the risk of stigmatizing the undocumented. In addition, the position is somewhat distant from the Cryola culture to the documentary mechanisms of citizenship. Many of them assume they don't want to have documents from « the white » and, at the same time, they clame for integration on the portuguese health, educational and social system.

2 - Theoritical framework

Medium, media, mediatisation: transmedia as a new (meta)medium [languages, images, narratives]

Transmedia is a relatively new concept linked to the development of Multimedia Technologies, to Media Convergence (whether business, technological, professional or communicative), to Interactivity, Multimodality and Multiplatform, among others.

For Rivera (2012) it is a narrative process based on the intentional fractioning of the content and its dissemination through multiple platforms, supports and channels (offline and online), so that each medium has a specific and complementary part of its content within the story in order to motivate the interaction with the user.

In short, it is about: 1) - a new form of story or narrative, 2) a working method of communications, advertising and marketing, 3) a process, 4) they are stories told through multiple media, 5) each medium tells a part of the story and what it does best, 6) the public or users are a fundamental part of this process to build, participate and disseminate the stories, 7) the TNs are the result of integrated production, and 8) the TN's are the result of a network of characters, events, places, times and means (Cfr. Scolari, 2013).

For Scolari "TNs are a particular narrative form that expands through different systems of meaning (verbal, iconic, audiovisual, interactive, etc.) and media (cinema, comics, television, videogames, theater, etc.)." (2013: 24). With this, "we are not talking about an adaptation from one language to another (for example from book to film), but a strategy that goes much further and develops a narrative world that encompasses different media and languages." (2013: 25).

In other words, transmedia narrative is a kind of story where history unfolds through multiple languages, media and platforms, not in the form of repetition, but in each experience the narrative expands, enabling new meanings and even new content thanks to the fact that consumers assume an active role in this process of creativity, dissemination and expansion. That is why we speak of prosumer (producer + consumer). Consequently, the logics of production, distribution and consumption differ from the typical ways of counting and producing stories and it is framed in what we can designate by digital culture

We consider digital culture in its "(...) specificity of the computational language and, consequently, of a new medium that promotes a communication paradigm to be considered in convergence, participation, ubiquity" and "(...) cultural practices translate the creative tension technology / message (...) "(Abreu: 2017 s / p).

3 - Methodology: Practice-as-research

This project is methodologically approaching artistic practices. Although we can anticipate some methodologies of more stabilized practices (for example the visual semiotics of Peircean tradition for the analysis of the illustrations in the "profiles" or platforms more related to the use of images (eg instagram) we will follow a methodology of practice-as-research present in the following protocol (criteria of the Arts and Humanities Research Council *apud* Easton (s / d): 4): a) Define a series of questions that will be dealt with in the course of the research; b) Specify a search context in which the starting questions are inscribed. Specify the importance of addressing these issues and the contribution made to knowledge of the subject's knowledge; c) Specify the methods used to deal with the proposed issues. Explain the choice and relevance of advanced methods.

4 - Reflection and assessment: *story world and participation bible*

4.1 – story world

The narrative master line has been the expanded understanding of the legal status of the human person promoting non-discrimination based on this status.

4.2 - Participation bible

Nevertheless the use of transmedia narratives were conditioned in their participatory registration, since in the context of formal education, participation is coercive, that is, the students' contribution is mandatory for the validation of the ECT's corresponding to the subjects Digital Anthropology and Cyberculture.

The central narrative of the project consists of a "life story" of an undocumented Cape Verdean living in Lisbon / Portugal. It is a classic approach to visual anthropology and results in an ethnographic video. The use of the platforms YouTube and Facebook aims to publicize this work although it promotes participation through *likes*, *shares* and *comments*. The use of radio and television broadcasting will tell stories of undocumented immigrants who have been expatriated to Cape Verde and who have come to realize it or not, socially and economically in their country of origin. The *Twitter* platform was used by a group of students to tell stories of denunciations of undocumented persons to authorities as a result of jealousy between boy/girlfriends. The *Instagram* platform would be used to narrate the changes in power relations of the family order resulting from the randomness of possession of documents. The story was told of an undocumented father who used the documents of the toxic-dependent son and who was ill-treated by him under the permanent threat of denunciation. The *blog "ka has dokumentu* » would relate separate stories related to the ontological nature of legal identity (for example, the case of twin sisters with age difference of 5 years or that of the minor who married with the documents of the recently deceased sister).

5 - Discussion and/or conclusions

The exploratory empirical research projects in progress are partial and the development of narratives depends on the domain of the potentialities of the different platforms. What has happened so far is that the game dimension and the creative competition among the Students has generated new ideas and different narrative strategies. The formal learning context in which the project is inserted can mitigate the participatory dimension of the project since the Students are conditioned by obtaining validation results in the disciplines involved in the project. Not being motivated by the process of fanitization NT's virtualities as a creative process to overcome the criolla condition in a multicultural context can result in reinforcement of the processes of self-esteem and validation of the identity process of the community.

6 - References

(1) Abreu, J. (2017). New medium, new poetry / nós raíz é la undi nóz biku sta interadu / entre identidade jurídica e liberdade poética. *V workshop internacional em Antropologia Visual e Novos Media*. Poster. Universidade de Cabo Verde, ISMAI – Instituto Universitário da Maia.

(2) Easton, L. (s/d). Rapport sur les méthodes utilisées en recherché artistique dans le domaine des arts de la scène, Manufacture – Haute école de théâtre de Suisse romande, In: http://www.hetsr.ch/index.php?option=com_content&task=view&id=869&Itemid=131

(3) Bertetti, P. (2014). Toward a Typology of Transmedia Characters. *International Journal of Communication* 8: 2344–2361.

(4) Fisch, S. M.; Damashek, S. & Aladé, F. (2016). Designing media for cross-platform learning: developing models for production and instructional design, *Journal of Children and Media* 10 (2): 238-247, DOI: 10.1080/17482798.2016.1140485

(5) Gambarato, R. R. (2013). Transmedia project design: Theoretical and analytical considerations. 2013. In: http://publications.tlu.ee/index.php/bsmr/article/ view/153

(6) Jenkins, H. (2003). Transmedia storytelling: Moving characters from books to films to video games can make them stronger and more compelling. *Technology Review*. In: http://www.technologyreview.com/biotech/13052/

(7) Long, G. (2011). We're Looking for Characters: Designing Personalities who Play Across Platforms. *Transmedia Hollywood* 2 [Panel discussion]. University of California at Los Angeles.

(8) Pratten, R. (2011). *Getting started in transmedia storytelling: A practical guide for beginners*. San Francisco, CA: CreateSpace.

(9) Rivera, D. (2012). *¿Qué es transmedia y storytelling?*, In: https://mediossociales.es/transmedia-y-storytelling/

(10) Scolari, C. (2008b). *Hipermediaciones. Elementos para una teoría de la comunicación digital interactiva*. Barcelona: Gedisa.

(11) Scolari, C. (2013). *Narrativas transmedia. Cuando todos los medios cuentan*. Barcelona: Deusto-Planeta de libros.

Authors

Name and surname of the first author Álvaro Elgueta Ruiz – Ph. D in Public Communication, Faculty of Science & Technology, Universidade de Cabo Verde (Uni CV).

Name and surname of the second author

José Abreu – PhD Student Digital Platform Information and Communication, Assistant at Universidade de Cabo Verde (Uni CV).