|  |  |  |  |
| --- | --- | --- | --- |
| Grifo UA preto | **University of Aveiro**  **2015.** | Department of Electronics, Telecommunications and Informatics | |
| Vedran  Semenski | SMARTIE – Secure and Smarter Cities Data Management | | |
|  | Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em (designação do Mestrado), realizada sob a orientação científica do Doutor (nome do orientador), Professor (categoria do orientador) do Departamento de (designação do departamento) da Universidade de Aveiro | | |
|  | texto Apoio financeiro do  (se aplicável) | |  |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  | texto Dedico este trabalho à minha esposa e filho pelo incansável apoio.  (opcional) |

|  |  |
| --- | --- |
|  |  |
|  |  |
| o júri |  |
| presidente | Prof. Doutor João Antunes da Silva  professor associado da Faculdade de Engenharia da Universidade do Porto |
|  |  |
|  | Prof. Doutor João Antunes da Silva  professor associado da Faculdade de Engenharia da Universidade do Porto |
|  |  |
|  | Prof. Doutor João Antunes da Silva  professor associado da Faculdade de Engenharia da Universidade do Porto |
|  |  |
|  | Prof. Doutor João Antunes da Silva  professor associado da Faculdade de Engenharia da Universidade do Porto |
|  |  |
|  | Prof. Doutor João Antunes da Silva  professor associado da Faculdade de Engenharia da Universidade do Porto |
|  |  |
|  | Prof. Doutor João Antunes da Silva  professor associado da Faculdade de Engenharia da Universidade do Porto |
|  |  |
|  | Prof. Doutor João Antunes da Silva  professor associado da Faculdade de Engenharia da Universidade do Porto |

|  |  |
| --- | --- |
|  |  |
|  |  |
| agradecimentos | texto O presente trabalho propõe-se divulgar as mais significativas técnicas de construção existentes em Portugal continental. O livro é composto por uma apresentação dos materiais tradicionais de construção (suas principais características), uma compilação de fichas técnicas (de carácter prático, uma vasta bibliografia comentada e um glossário de termos técnicos.  A importante colaboração de diversas personalidades ligadas à área da História da Arquitectura, bem como o levantamento fotográfico realizado contribuem para o conhecimento e valorização de um saber tradicional.  (opcional) |

|  |  |
| --- | --- |
|  |  |
|  |  |
| palavras-chave | texto livro, arquitectura, história, construção, materiais de construção, saber tradicional. |
| resumo | texto O presente trabalho propõe-se divulgar as mais significativas técnicas de construção existentes em Portugal continental. O livro é composto por uma apresentação dos materiais tradicionais de construção (suas principais características), uma compilação de fichas técnicas (de carácter prático, uma vasta bibliografia comentada e um glossário de termos técnicos.  A importante colaboração de diversas personalidades ligadas à área da História da Arquitectura, bem como o levantamento fotográfico realizado contribuem para o conhecimento e valorização de um saber tradicional. |

|  |  |
| --- | --- |
|  |  |
|  |  |
| keywords | texto livro, arquitectura, história, construção, materiais de construção, saber tradicional. |
| abstract | texto O presente trabalho propõe-se divulgar as mais significativas técnicas de construção existentes em Portugal continental. O livro é composto por uma apresentação dos materiais tradicionais de construção (suas principais características), uma compilação de fichas técnicas (de carácter prático, uma vasta bibliografia comentada e um glossário de termos técnicos.  A importante colaboração de diversas personalidades ligadas à área da História da Arquitectura, bem como o levantamento fotográfico realizado contribuem para o conhecimento e valorização de um saber tradicional. |

Table of content

[List of Acronyms I](#_Toc411517375)

[List of figures III](#_Toc411517376)

[List of tables IV](#_Toc411517377)

[1. Introduction 1](#_Toc411517378)

[1.1. Intro Part1 1](#_Toc411517379)

[2. State of the art 2](#_Toc411517380)

[2.1. IoT 2](#_Toc411517381)

[2.2. NoSQL databases and Big Data 2](#_Toc411517382)

[2.3. Access Control 2](#_Toc411517383)

[2.4. SMARTIE 2](#_Toc411517384)

[2.5. Related work 2](#_Toc411517385)

[3. Temporary 3 4](#_Toc411517386)

[3.1. Temporary 31 4](#_Toc411517387)

[3.1.1. Temporary 311 4](#_Toc411517388)

[3.1.2. hztfzurdtud 4](#_Toc411517389)

[References 5](#_Toc411517390)

[References (other) 6](#_Toc411517391)

# List of Acronyms

|  |  |
| --- | --- |
| ABAC | Attribute-Based Access Control |
| ACL | Access Control List |
| CC | Portuguese Citizen Card |
| CLI | Call Level Interfaces |
| DAC | Discretionary Access Control |
| DACA | Dynamic Access Control Architecture |
| DBMS | Database Management System |
| EKE | Encrypted Key Exchange |
| HDFS | Hadoop Distributed File System |
| IDAC | Direct Access Mode Interface |
| IDE | Integrated Development Environment |
| IIAM | Indirect Access Mode Interface |
| IoT | Internet of Things |
| JDBC | Java Database Connectivity |
| JVM | Java Virtual Machine |
| LDS | Local Data Set |
| LINQ | Language Integrated Query |
| MAC | Mandatory Access Control / Message Authentication Code |
| OCSP | Online Certificate Status Protocol |
| PDP | Policy Decision Point |
| PEP | Policy Enforcement Point |
| PSK | Pre-Shared Key |
| RBAC | Role Based Access Control |
| RDBMS | Relational Database Management System |
| SAAM | Secondary and Approximate Authorization Model |
| SDP | Secondary Decision Point |
| S-DRACA | Secure, Dynamic and Distributed Role-based Access Control Architecture |
| SPEKE | Simple Password Exponential Key Exchange |
| SQL | Structured Query Language |
| SRP | Secure Remote Password |
| SSL | Secure Sockets Layer |
| TFA | Two Factor Authentication |
| TLS | Transport Layer Security |
|  |  |

# List of figures

[Figure 1. Random Image 2](#_Toc411506059)

# List of tables

[Table 1. Temporary table 3](#_Toc411506264)

# Introduction

## Intro Part1

# State of the art

## The Internet of Things (IoT)

In this section the current state of IoT will be presented. The main areas that will be briefly presented and analyzed are: current state and overview, general concerns, recent work and studies, technologies used, implementation examples and expected future developments.

The IoT is a recent paradigm in the area of networks and communication that has had a lot of growth and new developments in recent years. Although there are a lot of definitions of the IoT and the somewhat changing and branching nature of the development trends in this area the basic and simplified idea of this concept is that nowadays everyday objects can be equipped with cheap microcontrollers, sensors, means of connecting to one another and the Internet. The devices can generally be divided into two categories: sensors and actuators, meaning that their purpose is to provide and share data or some kind of readings or to receive commands and react/complete actions accordingly. The overall implementation and use of this could be used in a number of applications including: home automation, industrial automation, medical aids, mobile health care, elderly assistance, intelligent energy management and smart grids, automotive, traffic management and many others [1] [2]. All of these offer beneficial and significant impact on almost all areas of everyday life and have potential for providing advancements in research areas unrelated to networking or computer science. The definition of IoT is not exact as the authors of [1] wrote. They explain that the two main views come from the name "Internet of Things". One vision views the concept from a network perspective concentrating on communication and connection problems while the other is oriented on the "Things" or object perspective concentrating on sensor technologies, new communication technologies like RFID and NFC ,and integration into other devices in a seamless and affordable way. A third view is also present which the authors defined as a "Semantic oriented vision" which is concentrated more on the use, implementation and processing of data.

A number of challenges are in the way of successfully building and utilizing the IoT. Scalability is one of the obvious challenges. Any kind of IoT application that requires a large number of devices commonly face problems with response time, memory, processing and energy constraints. Other challenges include security issues. The data being generated by sensor networks is huge and could over saturate the network, the data could be personal and as such has to be protected from unwanted access. Attacks by hackers, malicious software, viruses and other sources can also disturb the flow and integrity of data/information. As the authors of [3] [4] [5] describe in their work and stress the importance of security for a widely acceptable solution. In their work they describes the IoT divided into 3 or 4 layers and define security requirements for every layer providing the current state of technologies used in these areas. They stress the need for an uniformed and standardised open architecture and solution. Solutions for many of these problems are already conceptually known and are in some examples implemented but the lack of a open and standardized solution is certainly an issue that would proved to be beneficial if/when solved.

Technological advancements in various sensor modules and cheap and energy efficient microcontrollers along with recent communication technologies like RFID, NFC and network protocols are the main factors that enabled the fast development and spreading the IoT. Because of these advancements the concept became a reality and is gaining importance and more uses and applications. As the means of connection and communication are open and utilizes a number of older and newer technologies the networks and number of devices is fast growing and also brings up the problem of standardisation and implementation of standards in the purpose of uniformly solving known problems with for instance security, integrity and scalability.

A more future oriented view and analysis is provided by [6]. It describes a more human centric rather than thing centric future of the IoT. Devices being linked to people and monitoring their state and condition. Others are used for monitoring or controlling things in the environment but always in close relation to human needs and/or wants. It describes a need for IoT applications to provide better quality of service and seamless integration into areas of life. The more relevant and faster growing application domains are: Environmental Monitoring, Smart Retail, Smart Agriculture, Smart Energy and Power Grids and Smart Healthcare. The architecture proposed is separated into 5 layers stacked one on top another in this order:

1. Things - containing devices or elements that are data generators and/or consumers of information. The devices could range from small and unintelligent embedded systems to complex devices or virtual entities. The communication would be done different communication technologies and a wide variety of protocols.
2. Network - this layer contains functionality and means of managing a sensor network. Discovery of new devices, maintenance, scalability, universal abstractions of the Inputs and Outputs and general abstraction for the upper and lower layers and enabling plug-n-play like use using already known models like push/pull or publish/subscribe models and REST based protocols.
3. Data Management - it is defined as "Big-Little" Data Management referring to the data usually generated by sensor networks meaning that the data generated by for instance temperature sensors is small in individual reading size large considering a large number of sensors over a period of time. This layer is responsible for categorizing and aggregating data retrieved from the Network layer in order for it to be used and/or by the Analytics layer. Data generated by sensors is often slow changing so this fact should be taken advantage of for more efficient data storage.
4. Analytics - this layer mines/retrieves data from the Data Management layer and performs data processing and analysis depending on the type of data and end user of the result. Is provides the applications (which would be located on top) with useful data and information for subsequent use.

There a lot of commercial implementations of IoT on a smaller scale which are mainly focused on personal use in home energy consumption, health monitoring and environment monitoring applications. These solution usually utilize custom solutions along with custom hardware (regarding the sensor devices). Introducing standards that would be accepted and the creation of publicly available frameworks that utilize those standards would be very beneficial and would allow easier further developments. The lack of said standards and frameworks mean during initial developments of applications many of them face the same problems and implement a custom solution. This leads to incompatibility issues and stand in the way of a truly global IoT. The surveys and proposals given in [5] [3] give a good overview of the current situation in IoT and a give proposals for more uniformed future research and developments.

## Machine to Machine communication (M2M)

## NoSQL databases and Big Data

## Access Control

## SMARTIE

## Related work



Figure . Random Image



Table . Temporary table

# Temporary 3

## Temporary 31

### Temporary 311

### hztfzurdtud

# References

|  |  |
| --- | --- |
| [1] | A. I. G. M. Luigi Atzori, “The Internet of Things: A survey,” *Computer Networks 54,* p. 2787–2805, 14 June 2010. |
| [2] | N. B. A. C. V. M. Z. Andrea Zanella, “Internet of Things for Smart Cities,” 2014 April 2014. [Online]. Available: http://eprints.networks.imdea.org/id/eprint/740. [Accessed 12 February 2015]. |
| [3] | A. V. V. J. W. J. L. D. Q. Qi Jing, “Security of the Internet of Things: perspectives and challenges,” *Wireless Netw,* p. 20:2481–2501, 17 June 2014). |
| [4] | J. W. C. Z. J. L. Hui Suo, “Security in the Internet of Things: A Review,” in *International Conference on Computer Science and Electronics Engineering*, 2012. |
| [5] | A. R. L. G. A. C.-P. S. Sicari, “Security, privacy and trust in Internet of Things: The road ahead,” *Computer Networks 76,* p. 146–164, 15 July 2014. |
| [6] | Y. S. J. W. Prasant Misra, “Towards a Practical Architecture for the Next Generation Internet of Things,” 3 February 2015. [Online]. Available: http://arxiv.org/pdf/1502.00797v1.pdf. [Accessed 10 Februry 2015]. |
| [7] | R. B. S. M. M. P. Jayavardhana Gubbi, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems 29,* p. 1645–1660, 24 February 2013.. |

# References (other)

|  |  |
| --- | --- |
| [1] | A. I. G. M. Luigi Atzori, “The Internet of Things: A survey,” *Computer Networks 54,* p. 2787–2805, 14 June 2010. |
| [2] | N. B. A. C. V. M. Z. Andrea Zanella, “Internet of Things for Smart Cities,” 2014 April 2014. [Online]. Available: http://eprints.networks.imdea.org/id/eprint/740. [Accessed 12 February 2015]. |
| [3] | A. V. V. J. W. J. L. D. Q. Qi Jing, “Security of the Internet of Things: perspectives and challenges,” *Wireless Netw,* p. 20:2481–2501, 17 June 2014). |
| [4] | J. W. C. Z. J. L. Hui Suo, “Security in the Internet of Things: A Review,” in *International Conference on Computer Science and Electronics Engineering*, 2012. |
| [5] | A. R. L. G. A. C.-P. S. Sicari, “Security, privacy and trust in Internet of Things: The road ahead,” *Computer Networks 76,* p. 146–164, 15 July 2014. |
| [6] | Y. S. J. W. Prasant Misra, “Towards a Practical Architecture for the Next Generation Internet of Things,” 3 February 2015. [Online]. Available: http://arxiv.org/pdf/1502.00797v1.pdf. [Accessed 10 Februry 2015]. |
| [7] | R. B. S. M. M. P. Jayavardhana Gubbi, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems 29,* p. 1645–1660, 24 February 2013.. |