7

IoT in Brazil: An Overview From the Edge Computing Perspective

Marcelo Knorich Zuffo[1], Laisa Caroline Costa De Biase[1], Pablo César Calcina-Ccori[2], Catherine Pancotto Portella[3], Adilson Yuuji Hira[3], Gabriel Antonio Marão[4], Irene Karaguilla Ficheman[3], Geovane Fedrecheski[1] and Roseli de Deus Lopes[1]

[1]Escola Politécnica da USP, Brazil
[2]Instituto de Matemática e Estatística da USP, Brazil
[3]LSI-TEC, Brazil
[4]Fórum Brasileiro de IoT, Brazil

Abstract

In 2019, the Brazilian Government published the National Plan for the Internet of Things, which works towards fostering the development of this area in four priority environments: agribusiness, health, smart cities and industry. The plan also states that to establish a basis for solutions in these domains, investments in the following strategic fronts are needed: human capital, innovation, technology, and regulation.

We here summarize important scientific and technological advances in IoT, conducted by Brazilian institutions in the aforementioned strategic fronts: Code IoT education platform (human capital); Caninos Loucos SBC family and SwarmOS (technology); telecommunication regulation and the General Law for Personal Data Protection (LGPD) (regulation, security and privacy); and five applications (innovation) – Smart traffic lights, Smart surveillance, health monitoring of childhood cancer patients, Sleep apnea diagnosis, and Internet of Turtles. We also discuss regulatory aspects towards flexibilizing IoT services, and a recent law that protects the privacy of citizens in Brazil. These efforts clearly show a growing development of IoT in Brazil, particularly in areas that solve urgent problems, such as health and the environment.

Additionally, the existence of a national IoT platform leverages the massive creation of high-impact applications in the near future.

7.1 Introduction

The Internet of Things will dramatically change our lives, spreading connected computers with sensors and actuators, generating all sorts of smart things and producing enormous quantity of data, generating a whole set of new services. The potential socioeconomic impact of the IoT on economic productivity and improvements in public services in Brazil was estimated by McKinsey Consulting to be up to $200 billion – equivalent to approximately 10% of the 2016 Brazilian GDP. For example, in freight transport, real-time monitoring of goods could reduce costs up to 25% while intelligent choice of routes could reduce costs up to 20% [19].

Taking into account this context, the Internet of Things is considered an opportunity to the Brazilian industry to be positioned as a relevant solution provider in this segment. Since 2007, Brazilian stakeholders have monitored the segment transformations that started the IoT movement and have prepared to support the IoT ramp up.

Small technology-based companies are making moves to take advantage of that market. In 2016, there was a significant increase in the number of projects involving innovations in the Internet of Things submitted by startups to FAPESP[1] Innovative Research in Small Business (PIPE) Program. Just as an example, there are currently 21 projects led by startups from the state of São Paulo engaged in developing IoT solutions applied to things, such as health services, vehicle tracking, livestock management, building automation and energy management. Among them, we could mention Exati, a company in Curitiba, which has developed an IoT platform for a street lighting management system used in 200 Brazilian cities [19].

In 2019, the Brazilian Government published Decree 9854/19 establishing the Brazilian National Plan for the Internet of Things, in which an action plan was designed for the sector. This plan defined four fields of action: human capital, innovation, regulation and technology. This chapter presents some selected works in each of these fields from the edge computing perspective. The next section describes the Brazilian National Plan for the Internet of Things; one section is then presented to each of the fields of action. Section 7.3 presents the Human Capital field, presenting the Code IoT platform. Section 7.4 describes 5 IoT applications. In Section 7.5 we present the Caninos Loucos (hardware) and SwarmOS (software) platforms for IoT.

[1]The State São Paulo Research Foundation.

Section 7.6 shows some advances in IoT regulation. In Section 7.7 we discuss and present some concluding remarks for the chapter.

7.2 Brazilian National Plan for the Internet of Things

The Brazilian National Plan for the Internet of Things is a public policy that has been created by the Ministry of Science, Technology, Innovations and Communications (MCTIC) to sponsor the expansion of the IoT in Brazil. It refers to a set of strategies and public policies that seek to involve companies, the government and research institutions to disseminate the use of Internet-linked devices in Brazilian industry and services [1].

7.2.1 Priority Environments

The national plan selects technological niches and economic segments in which Brazil could have more ability to compete. As shown in Figure 7.1, four environments were given priority status for investments: Agribusiness, Health, Smart Cities and Industry. These environments were selected according to the existence of well-established companies in Brazil and in which there are good opportunities for developing innovations, with huge national demands.

The goal of each priority environment is described as follows:

- **Agribusiness:** to increase the Brazilian productivity and relevance in the global trading of agricultural products, with high quality and

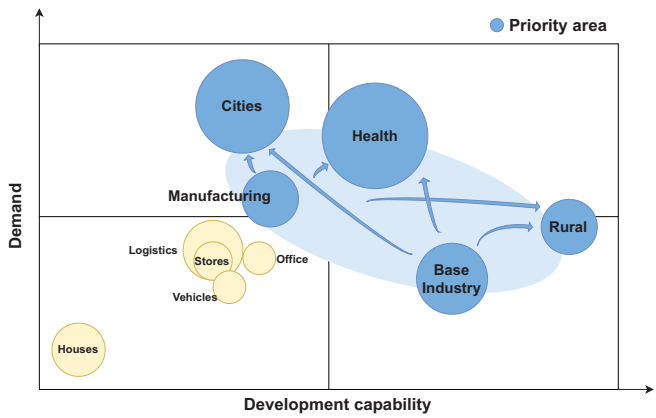

Figure 7.1 Demand × Developing capacity of IoT in Brazil.

Source: National Plan of IoT

sustainability, positioning the country as the largest tropical exporter of IoT technology.

- **Health:** to expand access to high quality health in Brazil, through health monitoring decentralization and increase in efficiency of health centers.
- **Smart Cities:** to enhance the quality of life of residents through technologies that allow integrated management of resources, and to enhance mobility, public safety, and resource usage.
- **Industry:** to foster the production of more complex items and to improve the national productivity through innovative business models and greater cooperation among various productive chains.

7.2.2 Main Structural Fronts

To achieve the goal of each environment, the plan is further structured in four main fronts: Human Capital, Innovation and International Insertion, Technical Infrastructure and Interoperability, and Regulation, Security, and Privacy. In the first front, **Human Capital**, the goal is to raise the potential for building IoT solutions, while directly benefiting the population through courses, grants, and other public policies. Some challenges to be addressed in this front include the enhancement of basic education and better integration of industry and academy, and how to quickly train and to attract high-quality professionals to serve the demand that IoT will incur. A particularly successful initiative in this respect is the CodeIoT program, which offers six free Massive Open Online Courses (MOOC) and has taught over 50,000 students, most of which were not previously introduced to programming or electronics, on how to build IoT solutions.

The **Innovation and International Insertion** front seeks to develop new IoT platforms and applications, while also making them stand out in the global landscape. It includes public financing to develop pilot projects in the most relevant environments, and enhancing competence centers to develop IoT enabling technologies, such as hardware and software platforms. Some pilot projects are already being developed, including a platform for smart management of traffic lights with low cost communication, and health monitoring of children with cancer. Finally, this front will also create an IoT Observatory, to facilitate tracking IoT development in Brazil and sharing news and other initiatives carried by the national plan.

Another front comprises **Technical Infrastructure and Interoperability**, and its main goal is to foster the development of open IoT platforms to support the creation of advanced and interoperable applications, as well as to facilitate the development of connectivity solutions. Regarding the

development of open platforms, the Caninos Loucos program stands out as the official platform for Single Board Computers within the national plan, while the SwarmOS is a new software platform for decentralized IoT applications. Finally, the **Regulation, Security, and Privacy** front aims to adjust the regulation to facilitate IoT adoption, while keeping risks of new technologies as low as possible and protecting the personal data of its users. A significant challenge resides in minimizing the impact of impositions set by existing telecommunication regulations over new business models and services offered by IoT applications. Advances in this regard are being made by the National Agency of Telecommunications (Anatel), which seeks to flexibilize regulations and encourage IoT adoption. Data privacy and security also faces challenges, as the IoT significantly increases the points for data collection. While the General Law of Personal Data Protection (LGPD), issued in 2018 by the government, may be a starting point for protecting privacy, more work has to be done, especially regarding security risks and certifications.

To enforce the execution of the national plan, a Chamber for Management and Monitoring of Machine-to-Machine and Internet of Things Communication Systems Development (Câmara IoT) was created [1]. The new chamber is composed by members of the MCTIC, the Ministry of Economy, the Ministry of Agriculture, Livestock, and Supply, the Ministry of Health, and the Ministry of Regional Development. Members from other public and private associations may also be invited to contribute to the Chamber.

The Brazilian National Plan for the Internet of Things is serving as a catalyst to foster value generation throughout the country, which ultimately benefits companies, users, and society as a whole. The following chapters describe selected scientific and technological advances in the fronts and environments aligned with the plan.

7.3 Human Capital: The Code IoT Project

Considering the global importance of IoT and the way it is already changing our lives, it is important to encourage new generations of engineers and computer scientists to learn and to study different aspects of Internet of Things. This stimulates the solution of problems and development of solutions that improve agribusinesses, health, cities and industries. This topic is widely addressed in undergraduate and in graduate courses, but not necessarily in K-12 (basic education) environments, especially with high school students who can understand the concepts, start developing simple solutions, eventually choose STEM careers and, in the future, contribute to creating intelligent IoT applications.

Seeking to bring basic education students closer to the concept of Internet of Things and programming tools, physical computing and application development, we created the Code IoT platform with free online MOOCs in different aspects of IoT.

7.3.1 Methodology

Initially we conducted a face-to-face activity with 32 high school students and their teachers when we offered a 16-hour IoT workshop. The activities were structured to engage students in creative construction and learning processes based on project-based learning strategies and aimed to modify their understanding of the technologies they already use, as well as their ability to create conceptual IoT solutions and to implement simple initial prototypes.

Activities related to programming, physical computing, and robotics have been offered to K-12 students due to the development and dissemination of new tools suitable for use by children and teenagers. Working with these themes enables engagement in interactive, dynamic, and multidisciplinary learning activities that can contribute to increased motivation and assimilation of scientific, technological, mathematical, artistic, and engineering concepts in solving real-life problems.

During the workshop, we filmed, photographed and observed the students and their teachers. We also interviewed and collected feedback from the participants.

Based on the IoT workshop experience and the feedback analyses, we created the Code IoT platform available at www.codeiot.org.br with six online courses that present and discuss several aspects of IoT:

1. **Introduction to IoT.** This is a theoretical course that presents basic concepts of Internet of Things, explains what it is and how it works, shows some of its applications that are already part of our daily lives and explains tendencies in this area.
2. **Learning to code.** In this course, users take first steps in the universe of programming. Using the programming language Scratch, they have the opportunity to create projects involving stories, animations and games, to interact with the online Scratch community and to learn important programming concepts in a practical way.
3. **Electronics: concepts and basic components.** This course explains how an electric circuit works and how to create circuits with electronic components that are easily found. Users get familiar with electronics concepts that will help them understand how things work. They also

learn how to assemble a basic electronic kit to take first steps in projects construction.

4. **Physical computing.** In this course, users learn how to create projects using microcontrollers capable of interpreting information from the environment and able to execute actions in the physical world. They understand how some of the electronic devices that we see around us work and learn how to create intelligent objects, integrating programming and electronic circuits.
5. **Apps for mobile devices.** This course approaches apps creation. Users practice and explore concepts that are behind the operation and creation of Smartphone apps. They learn to develop programs and interfaces, using AppInventor. They get familiar with design and usability aspects that are important in mobile application development, and they create their own apps and see them running on their Smartphone or tablet.
6. **Intelligent Connected Objects.** This course integrates electronics, programming and Internet of Things knowledge to create solutions for real world problems. Users have the opportunity to use what they have learned in previous courses to create solutions for real world problems connecting various technologies. They create and develop intelligent objects able to communicate with Smartphones and interact with the environment.

7.3.2 Implementation

The Code IoT platform was launched in September 2017. The six courses are free online MOOCs and have been offered several times since then, typically 2 to 3 times each year. The courses are six-week long and demand a 4 to 6-weekly-hour effort. All the courses are based on Problem-Based Learning paradigms and always end with a project the users have to create and to submit. Participants that conclude all the tasks proposed receive a certificate for each course. Courses are intended for basic education students and teachers; however, anyone interested in the subject can enroll.

In 2017, the courses were all in Portuguese, and in 2018, the courses were translated into Spanish and English and have been offered simultaneously in the three languages since then. In three years (September 2017–September 2020), the platform has had 105,579 registered users, counts on 212,233 enrolments in the courses, issued 9,414 certificates totalizing 169,796 training hours.

After analysing the users profiles, their age and occupation, we observed that most users were university students (undergraduate and graduate) and

professionals interested in the IoT subject. We then started to work with high school teachers in face-to-face workshops, for them to be acquainted with the Code IoT platform, to conduct interactive activities with their students and to encourage them to engage in the online courses. In two years (September 2017–December 2019), we conducted 21 workshops in two Brazilian cities, in which 1,228 teachers participated and have impacted 9,233 high school students.

7.3.3 Future Work

We intend to continue our effort in promoting human capital development by intensifying the promotion of the Code IoT platform with High School teachers and students and conducting face-to-face workshops.

We are also planning to attend undergraduate and graduate students creating new MOOC courses on IoT and the Caninos Loucos hardware platform as well as the IoT middleware software called SwarmOS.

7.4 Innovation: IoT Applications in the Brazilian Industry

In this section, we describe some ongoing efforts towards the solution of problems of high interest in Brazil, such as health, traffic, urban surveillance for security, and environment. The first four applications are the result of a consensus amongst several research, industrial, and government institutions under the program of IoT National Pilots developed by the Brazilian Development Bank (BNDES). Those projects will take place in the beginning of 2020 and will have a great impact on the solution of the above listed problems. The *Smart traffic lights* project proposes installing edge devices in the traffic lights of São Paulo city, for better traffic light control. The *Smart surveillance* project will put mobile cameras with computing abilities for capturing hazardous scenes through computer vision algorithms. The *Health monitoring of cancer patients* and *Sleep apnea diagnosis* projects aim to use IoT devices to monitor the health of patients in order to perform early diagnosis and save lives. The rest of this section presents further details about these projects.

7.4.1 Smart Traffic Lights

The project aims to implement and to evaluate a network of smart traffic lights with remote programming through a Fixed-Time Traffic Light Control

Center, aiming to offer tools to improve the effectiveness and efficiency of urban traffic management. IoT devices built into the fixed-time traffic light controllers will be used to establish a wireless communication network between the control center and the controller, allowing their remote reprogramming and monitoring.

Smart transport is a priority for São Paulo city, especially in improving the modal fluidity. Brazil currently loses approximately $156.2 Billion with traffic jams in the city of Sao Paulo. Traffic light controllers have a fundamental contribution to traffic. In the city of São Paulo, there are about 6,000 traffic lights. Among them, 4,500 operate in fixed time; in other words, configured to operate following a temporal schedule. The remaining 1,500 traffic lights are real-time, remotely controlled by a fibre optic network, determining the state of the traffic lights at each instant.

Between 1993 and 1997, five real-time Area Traffic Centers (CTAs) were implemented in the City of São Paulo. Five CTAs were required instead of one because of a restriction that each manufacturer's semaphore controller model could only be installed in their respective CTAs. This restriction not only increase the required investments to operate the system but prevents integration. Thus, CET began a search for solutions that would allow semaphore controllers from any manufacturer to be connected to CTAs with standardized and open communication protocols.

Currently, the São Paulo Traffic Engineering Company (CET) does not yet have a Fixed Time Traffic Light Control Center; configuration changes or problem identification and remediation require CET teams to be relocated for reprogramming or recovery, resulting in a high operating cost and low agility in problem-solving. There are great opportunities for system improvement, since the identification of non-working traffic lights is mostly received by citizens' complaints, and the average time between receiving a notification and troubleshooting is 9 hours. Thus, remote access to fixed-time semaphore controllers is currently a demand, as it would lead to improving the system availability and the fluidity of transport modes, especially in adverse or peak usage situations.

Taking advantage of IoT technologies for remote programming and diagnosis of traffic lights, the project aims to connect Fixed-Time Traffic Light *Connected Controllers* to a Fixed-Time Traffic Light *Control Center* through a standardized and open communication protocol. The IoT solution is divided into three main layers: devices, network, and application; a fourth layer permeates all the others: security.

- Device layer: comprises the Fixed-Time Traffic Light Connected Controllers, which are able to receive remote updates to its local database of traffic light schedules. These devices can also notify the Control Center about any emergency or problem detected in the traffic light function;
- Network layer: pursuing the flexibility of semaphore controllers manufacturers, the use of a standardized and open communication protocol is mandatory. The solution will use an event-oriented IoT messaging protocol and a long-range, low-cost, IoT-suitable communication, such as LoRaWAN, which uses sub-gigahertz frequencies for extremely energy-efficient data transmission over distances of up to 10 km. One of the technical and scientific challenges faced in this project is the potential size of the configuration packages, which must be optimized to fit within the communication mechanism bandwidth requirements;
- Application layer: comprises the Fixed-Time Traffic Light Control Center, which will be developed using open source software, commissioned by the municipality but not yet validated in the field.
- Security layer: appropriate and well-established protocols will be implemented for each device, network and application. As the traffic management, more specifically traffic lights control, is a critical mission, security is of major importance.

7.4.2 Smart Surveillance

According to the Numbeo[2] ranking, Brazil is the 7th country in the world with the highest rate of criminal occurrences. In Latin America, Brazil is only behind Venezuela, which leads the global ranking. In addition to direct damage to the impacted population, the effect of violence on the country's economy can cost 3.14% of the GDP, according to estimates by the Inter-American Development Bank in 2014. In order to be more effective in combating crime, law enforcement agencies focused on the use of technologies, among which, the use of fixed cameras installed in several cities in Brazil to reduce costs and to increase effectiveness in combating risk situations to citizens. However, despite the benefits provided by fixed cameras, their static nature limits their coverage of specific areas. In addition, criminals can simply change the place of operation. If safety for all is a goal, solutions that are more effective have to be introduced.

[2] www.numbeo.com

A major benefit of the Internet of Things is that it can transform any object in the physical world into an information retriever and transmitter. In this context, this project proposes creating a mobile sensing network by installing IoT devices in vehicles, since they provide natural mobility, increasing the coverage area and reducing the chance of being predicted by criminals. Another benefit of vehicular sensing lies in the possibility of not simply detecting crimes, but detecting life-threatening situations in general, such as accidents.

If the effectiveness of police in fighting crime depends on a widespread surveillance, success in emergency response is particularly impacted by its speed, because the faster the help is provided, the greater are the victims' survival or criminal apprehension chances. Currently, the State of Sao Paulo emergency notification system is based on telephone calls, which depend on people contacting, explaining the occurrence and giving the location of the incident. Only after this process is completed is the emergency service able to allocate a resource for the call. Since individuals involved in emergency situations may be disoriented or unconscious, an automatic, geolocalized, and reliable notification may save lives.

The pilot will use a device capable of reading and notifying vehicle license plates (Sentinel), which will be installed in a car fleet to perform the system evaluation in the field. The pilot fleet used in this pilot will consist of 50 cars from the Police force and 10 volunteers' cars. A module to receive the notifications from IoT to be integrated in the PM Operations Center (Central), will also be implemented; it will include the notification of accidents involving vehicles and the license plate readings. For the accident reporting assessment, the Sentinel will simulate the incidents. The IoT solution is divided into three main layers: devices, network, and application; a fourth layer will permeate all the others: security.

- Device layer: comprises the Sentinel, which will build on a pre-existing computing platform, the Labrador Single Board Computer (SBC), and incorporate the necessary communication sensors and modules;
- Network layer: the project will use LoRa, a low-cost and long-distance protocol for IoT communications;
- Application layer: comprises data management, storage, and analysis tools, and includes APIs for receiving incident notifications;
- Security layer: considering the sensitivity of the transmitted information, such as license plates and data about criminals, the confidentiality and integrity of the exchanged messages is critical.

7.4.3 Health Monitoring of Childhood Cancer Patients

The spread of Mobile Devices has sparked a new era of possibilities for IoT-based healthcare solutions. Future generations of IoT solutions promise to transform the healthcare industry by enabling breakthrough computing and communication capabilities, where individuals are monitored online by connected wearable sensors, enabling interoperability of personalized health and wellness-related information, patient's vital parameters, as well as data on physical activity, behaviors, and other critical parameters that affect daily quality of life.

Infections represent the main immediate cause of death among children undergoing cancer treatment. As the first symptoms of infection appear, immediate referral to their Health Service Center is absolutely vital, fever being the main symptom.

The context of the project is to monitor the patient's body temperature remotely, transmitting its readings through Bluetooth Low Energy to a smartphone, which stores and sends this data to a cloud-hosted web service via 4G wireless network. This allows the treatment center and the treating physician to receive alerts and monitor the temperature of their patients in real time from a computer, tablet or smartphone. The main objective is to develop and to analyze the use of wearable sensor-based IoT technologies for monitoring vital signs of people, specifically temperature in Child Cancer patients.

The focus of this study is to evaluate the mentioned platform as a precise tool for detecting the infectious condition, allowing the notification of patients and caregivers, which will allow immediate referral to the clinical treatment service in the emergence of fever symptoms, and to analyze their evolutionary impact in this process.

This project uses an IoT platform called Caninos Loucos Pulga, being developed under the National Microelectronics Program of MCTIC, for constructing microsensors based on micro PCB (Printed Circuit Board) Shield. The clinical study will be conducted at the ITACI – Child Cancer Treatment Institute, HC-FMUSP – Pediatric Oncology Treatment Service at the University of São Paulo, accredited by the State of São Paulo Health Department (SES-SP). This project will be implemented in the 2020–2021 biennium.

7.4.4 Sleep Apnea Diagnosis

Currently, for diagnosing sleep disorders, there is the all-night polysomnographic study performed in laboratory, which is the gold standard method for

diagnosing sleep disorders. The polysomnographic study allows recording several parameters: Respiratory effort through Inductive Plethysmography Chest Strap, Nasal Flow for Pressure Measurement, Oxygen Saturation (O_2), and Heart Rate.

Although polysomnography is considered the gold standard method for diagnosing sleep disorders, it is necessary to expand diagnostic methods, since not all patients have access to polysomnography, as it is an expensive exam. Moreover, there are Brazilian cities that have no doctors trained in sleep medicine and no laboratories or sleep clinics.

Apnea is currently the most prevalent sleep disorder in about 32% of the population. Thus, providing an affordable Sleep Apnea diagnostic test would bring enormous social and public health benefits as an alternative to polysomnography. In addition, an IoT-based Sleep Apnea diagnostic test would allow patients from remote locations to be monitored and diagnosed remotely.

The objective of this work is developing a sleep quality monitoring system to provide a solution for diagnostic test Sensors with IoT technology, directed to diagnosing Sleep Apnea. An important effort to enable proper monitoring in this work is Signal Characterization and Pattern Recognition for Apnea Diagnostic Calibration by IoT Sensors in relation to Polysomnography measures.

IoT Sensor exams represent an alternative to polysomnography for its ease of access and dissemination, provided there is a network connection, as well as its low cost, besides being an appropriate approach to meet a public service demand. While sleep disorders, such as Apnea, currently affect a large portion of the population, these patients do not currently have access to adequate services due to the lack of an affordable diagnostic test. This project also will use a platform called Caninos Loucos Pulga[3].

This clinical study is conducted at the Sleep Institute (Instituto do Sono), a reference center for sleep disorder care. It is associated to the Federal University of São Paulo (UNIFESP).

7.4.5 Internet of Turtles

In the last 50 years, the growing expansion of coastal cities in Brazil increased sea pollution and exploitative hunting, which threatens some turtle species.

[3]Pulga literally means *flea* in Portuguese.

Monitoring those individuals helps to protect them; however, several technical challenges arise. First, turtles spend most of their time under the ocean, which deteriorates the materials of specialized equipment. Second, seawater high conductivity is a problem for electronic equipment. Third, the considerable distances traveled by turtles require long-range antennas to cover such large areas.

Some initiatives, such as the Tamar Project[4] and the Guajiru NGO seek the preservation of turtles in critical regions on the Brazilian coast, such as Ubatuba (SP), Salvador (BA), and João Pessoa (PB). Actions by these institutions include protection of new-born turtles, preservation of their ecosystem, and sustainable development of local communities. Monitoring living specimens is paramount, and technology plays an important role in this task.

To provide a technical solution for the monitoring problem, the Internet of Turtles project is an ongoing effort developed by the University of São Paulo in collaboration with the Tamar Project and the Guajiru NGO. The objectives of the Tamar project include developing an electronic device to monitor turtles that satisfies the environmental constraints. These constraints include minimum size, low cost, lightweight, and long-range communication capabilities.

Two key technologies to implement the Internet of Turtles project are: the Caninos Loucos Pulga single board computer and the LoRaWAN network protocol. The Caninos Loucos board family is described in detail in Section 5.1; it includes the Pulga chip, whose physical size and energy consumption are low. Accordingly, the LoRaWAN network protocol provides long-range transmission of small data packages, besides using Sub-GHz communication, which is highly efficient for distances over 10 km. The Internet of Turtles project also comprises the research of software-defined radios to be integrated into the Caninos Loucos Pulga chip.

Turtle monitoring will be achieved by embedding the developed device into turtle shells and sea buoys. The support from the Tamar Project and from the Guajiru NGO will be of great importance for deploying the system.

7.5 Technical Infrastructure and Interoperability

This section describes two complementary efforts towards a unified IoT platform for the Brazilian market. It consists of a hardware platform called

[4]https://www.tamar.org.br

Caninos Loucos[5] and a software IoT middleware called SwarmOS. Together, both technologies provide a full stack platform that leverage local innovation in diverse IoT application areas.

The Caninos Loucos is a program to design and to deploy a family of single-board computers, whose development was the result of several factors, among which are the high taxes for importing hardware technology in Brazil. The Caninos Loucos has evolved since then, from the Labrador SBC to a whole family of boards ready for industrial applications.

The SwarmOS is a bio inspired IoT middleware that creates a decentralized network of heterogeneous devices, mediates the communication, and facilitates resource sharing across devices. The Swarm constitutes the natural complement for the Caninos Loucos hardware platform, as both work in tandem to provide a full platform for the future IoT.

7.5.1 The Caninos Loucos Hardware Platform

Single Board Computers, or SBCs, are complete computers integrated into a single printed circuit board. They usually have very small dimensions, close to the size of a credit card, and affordable cost, of the order of a few dozen dollars. Despite their reduced size and cost, SBCs are very powerful computers at low power consumption, incorporating multiple input and output interfaces of General Purpose I/O (GPIOs), wireless and wired Internet connection, USB ports, sensors and actuators. With the evolution of technology, SBCs have become an essential platform for developing Internet of Things and Industry 4.0. In recent years, there has been a proliferation of marketing models and volumes that exceed millions of units sold in many countries, such as SBC Raspberry PI designed and manufactured in the UK. In this context, we present the Caninos Loucos Program, which aims to: specify, design, develop, manufacture and market a family of Open SBCs fully developed in Brazil and in Latin America. It also aims to develop SBCs focused on the needs of the maker community and, at the same time as the local industry, to promote the development of IoT initiatives in Industry 4.0, from the availability of a development platform that can be easily modified and adapted to the needs Latin American regions. This project is part of the current National Plan for Internet of Things, promoted by the Brazilian Federal Government. Moreover, the Caninos Loucos Family has covered all levels of application in edge computing, starting from smart sensor nodes to

[5]Caninos loucos literally means *mad dogs* in Portuguese.

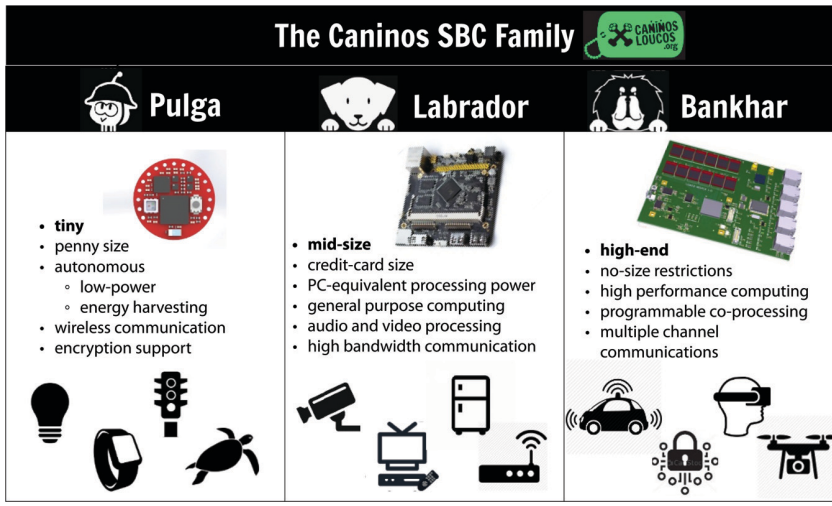

Figure 7.2 The Caninos Loucos single-board computer family.

high end performance computers. Figure 7.2 provides an overview of each member of the family with their main features and usages.

7.5.1.1 Hardware requirements at the edge

Edge computing consists in having most, or even all, of the processing work happening at the site, instead of in the cloud, to improve responsivity and reduce bandwidth use. To meet this requirement, the edge-based systems, or smart objects, as they are called, need to have embedded electronics with a considerable processing power, memory capability, reliability and scalability. In this sense, the hardware has to be robust in terms of both energy and security, to be able to communicate with other systems ensuring interoperability and, finally, being able to process the data in a reasonable time. Also, power consumption is very critical at the edge since many of the applications involve energy constraints, especially the ones related to agriculture and medical applications. In this sense, having a long battery life option is essential for the platforms that work at the Edge. Lastly, it demands both short- and long-range communications for most of its applications and a large variety of communications are used at the edge, such as Wi-Fi, LoRaWAN, BLE, Sigfox, Ethernet and others.

Therefore, the supply of smart objects will depend on the design of electronic systems. Electronic system designs may be developed with a variety of strategies that will impact: the cost of the project (non-recurring

engineering cost) and the time to market. The system design can range from a totally dedicated project, even including the design of a new electronic component (ASIC), to the use of a ready-to-use computational module. This also facilitates the integration of computing devices to smart objects by companies not previously familiarized with electronics and the demand for personalized products, with specialized batches in lower quantity.

7.5.1.2 The need for an open SBC platform

To meet the demands of edge-based systems, the single board computers present the opportunity to consolidate products with smaller time-to-the-market, since SBCs are essentially compact computational modules, that are expandable, scalable and with a variety of configurations, processing performances and costs. Therefore, it can also significantly reduce the non-recurring engineering costs involved in an IoT project. These costs represent the investment on the development itself, including hardware and software, in cases of embedded electronic products; by using the SBC one can minimize the hardware project cost by using a known platform and focus on the software design. This approach will save both the time and money spent in development. In this sense, SBCs establish a paradigm of computer as a device, which allows it to be embedded in practically anything anywhere.

Hence, SBCs are ideal platforms for IoT and edge computing solutions, since edge computing consists in taking most of the processing work to the edge instead of the cloud. The latter requires a combination of powerful processing and low power consumption, which SBCs already have, since they are largely used in embedded systems; for that, they need to have extended working life as well as the capability of having communication according to the application of use. Moreover, the extended fields of usage of the SBCs demand a high number of peripheral possibilities and variable memory capability. Therefore, hardware requirements vary with the application but in general the SBCs have enough processing capability to handle most, or even all, of the computing load of the system. Besides, SBCs that implement DSP instructions and cryptography hardware acceleration ensure the security in edge computing systems.

Moreover, since each application has its own requisites, the versatility of SBCs is important. They have as many peripherals as possible, such as wireless communication, I2C, SPI and other interfaces to communicate with other components or with the external world. Finally, the strategy of using SBCs in edge computing allows a variety of peripherals and communication protocols needed in smart systems development with the advantage of low

development costs, low time to market. Besides, they ensure the security of the system by not having backdoors or allowing industrial espionage, since they can be customized for each application, provide economy to the overall project due to the lower prices and taxes, and also integrate it on the IoT wave.

7.5.1.3 Caninos Loucos family as a platform for edge computing

The SBC Caninos Loucos presents several innovations, such as internal processing, low energy consumption, optimized communication protocols for the Internet of Things, adaptability to different processes, high concern for information security, ease of use, and an open and collaborative approach to projects. For greater versatility and appropriateness to this concept, the family uses a two-board strategy: an IoT core module consisting of the computational (CPU and Memory) unit and a base board with interfaces and peripheral support. This flexibility of the proposed platform is a differential; it will generate a standardization of pinning and a printed circuit board architecture that will allow meeting various demands by business, start-ups and inventors.

The two-board strategy enables the Caninos Loucos SBC to work as platform for edge computing since its main board contains a powerful processing module associated to a base board that can be customized, allowing versatility on power and communication, the two main restraints in edge computing applications. Moreover, the standardization of the pinning permits users to change the computing module according to the processing needs of the application while maintaining the peripherals on the BaseBoard or vice-versa.

The Caninos Loucos Family has different boards for different uses, while maintaining the two-board concept. In this sense, the development of the Caninos Loucos family aims to cover three categories of applications, according to computing capabilities: SBC-tiny, SBC-mid e SBC-high. Figure 7.2 summarizes the main characteristics of the Caninos Loucos board family.

The first SBC in the Caninos Loucos Family is the Labrador, which focuses in the *SBC-mid* category and includes credit card-sized boards (8.5 cm $\times$ 5.5 cm) or 46.75 cm^2. Applications for this board family include communication gateways, microservers, personal computers, embedded boards in white-good appliances, educational toys, among others, since it can run Linux and Android and access the internet via cable or Wi-Fi. It has enough processing and communication power to process high resolution audio and video. Thus, it is a miniaturized generalist computational platform, with computing power equivalent to a low-performance personal computer

and size close to a credit card. These platforms bring versatility and agility to a wide range of applications, including thin clients, home appliances, security cameras, set-top boxes, gateways, etc.

The IoT module, called Labrador Core, contains the processing unit, the power management unit and the volatile and non-volatile memories. These components are highly sensitive to impedance variations and demand high speed signals, which implies a more complex and sophisticated project. The baseboard, called Labrador Base, has a simpler design, with lower frequency signals and simpler components. This strategy is appropriate to the open hardware approach, since it consolidates two projects with very different redesign difficulty level and with software compatibility, since a single module can be used with different baseboards customizable according to each application. Figure 7.3 shows a Labrador SBC with the IoT module and the BaseBoard, designed and produced in Brazil.

The second SBC in the family is the Pulga, the Tiny SBC that comes to meet a demand regarding the trend of distributed processing using the edge computing approach since many IoT designs are strongly centered in the cloud, with low processing power being demanded by the device itself. It constitutes a single board computer, with considerable processing capacity, yet at low cost, small size, which is versatile in communication mechanisms and sensors but with high autonomy. The device high autonomy is achieved using low-power components associated with an energy-harvesting circuit and optimized software for low-power consumption. Its design adopts

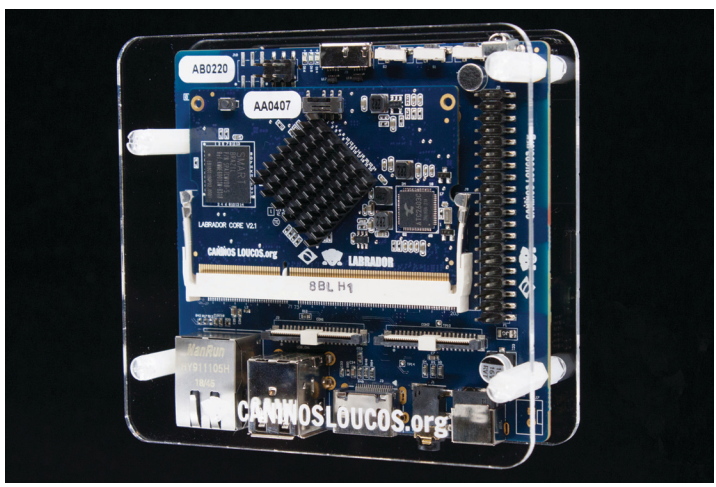

Figure 7.3 The Labrador single board computer.

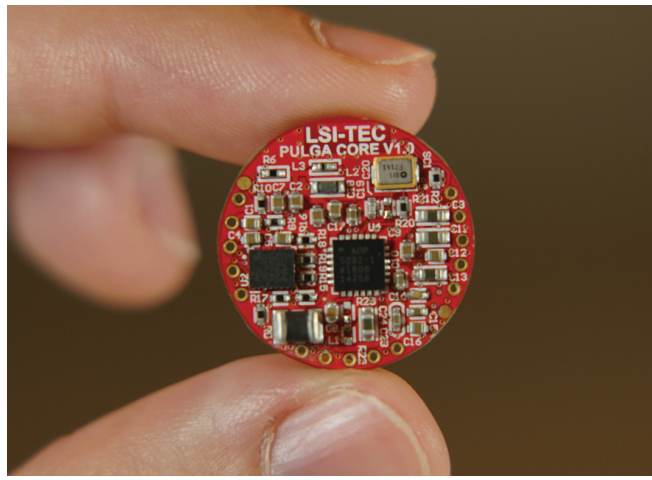

Figure 7.4 The Flea single board computer.

new communication standards for low-range communications allowing the constitution of mesh networks of more than one thousand nodes, which is particularly interesting for sensing and monitoring applications. The *SBC-Tiny* family is targeted to last-mile edge computing, where connectivity, computing capabilities, and energy consumption are extremely limited. The size of these boards is less than 2 cm^2 Applications for these boards include sensors and actuators for diverse areas, such as agribusiness, home and industrial automation, health, fitness, entertainment, and wearables. Figure 7.4 shows a Flea SBC in its initial version, manufactured by LSITEC in Sao Paulo, Brazil.

Finally, the *SBC-high* family proposes high network computing performance as the main characteristic, cable of reaching a 1 Teraflop of processing power with much lower consumption than other high-end solutions. Potential applications of this family are autonomous vehicles and virtual reality engines, among others.

7.5.2 SwarmOS

The term swarm was first proposed [2] to refer to sensory found at the edge of the cloud, and identified the opportunity for materializing/serving areas such as cyber-physical systems, cyber-biological systems, immersive computing and augmented reality. Subsequent work led to a more concrete definition of the Swarm, particularly the proposal of an initial architecture

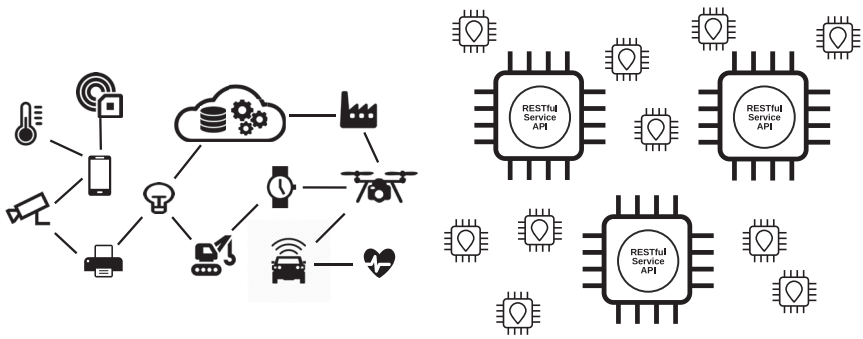

Figure 7.5 The SwarmOS architecture.

for the Swarm [3] in the context of a larger project called TerraSwarm. They also outlined a common framework for devices to communicate and to share resources, called SwarmOS. The architecture of the SwarmOS framework was further developed [4], complementing the already existing distributed storage system (*data plane*) with a module responsible for sharing and managing resources (*control plane*).

The Swarm is a self-adaptive network for autonomous smart objects. Devices do not rely on the cloud for storage and processing; instead, part of this work can be performed in the device itself. The Swarm is a heterogeneous network constituted of different kinds of devices, with variable computing power and energy capabilities. In Figure 7.5, we illustrate the general structure of the Swarm. Making a parallel with swarms of bees, with specialized bees contributing to a common goal, the Swarm is composed of specialized devices whose interaction solves a common problem. The Swarm network behaves as an organism and shows an organized behavior resulting in an emergent collective intelligence.

7.5.2.1 The Swarm architecture

Device functionalities are exposed to and shared with the network as *services*. Thus, the Swarm can be seen as a large network of interacting services. Every service is specialized in a specific functionality, and many services can perform similar or equal functionalities. The true potential of the Swarms resides in the composition of services, which dramatically extends the functionalities offered by the network. Given the intersections with the *microservice* architecture style, we adopted many of its concepts for the Swarm, such as the use of services as the main building block; loose coupling and high cohesion;

decentralized governance; decentralized data management; and evolutionary design [5].

Interaction among devices is performed opportunistically, with no prior agreement. The connection among devices is established in real-time, based on the availability of devices in the network. As a response to an external event, devices in the network form groups to perform an action or to give an answer. Although those groups formed are transient, the success of each interaction is recorded in the network and serves to build a measure of *reputation* for each device. The Swarm platform is based on a lightweight middleware installed in every IoT device called SwarmBroker, which acts as a communication facilitator. Some functions provided by the SwarmBroker include registry and semantic discovery of services in the network, enforcement of policies for access control, a decentralized mechanism for service contracting and reputation, based on blockchain. The transaction model creates contracts between service consumers and providers which are chosen by a combination of price and reputation, thus creating an economic model for resource sharing in the IoT.

7.5.2.2 The SwarmBroker

The actual software framework that implements our Swarm vision is called *SwarmBroker*. It acts as a facilitator of communication among services. We define two categories of services in the Swarm: *platform service*, which constitutes the core functionalities of the Swarm network; and *application services*, all other services that participate in the Swarm. Platform services include *discovery* of other services; *registry*, a distributed catalog of services; *access control*, which determines the access to resources; *binding*, which translates commands among protocols; *policy management*, a repository of policies used by access control; *contracting*, which establishes service-level agreements for the use of services; *mediation*, which offers a semantic support for discovery service; and *optimization*, which analyses data generated by device interaction to tune network parameters and policies. The Broker can be seen as the collection of platform services. Figure 7.6 illustrates the landscape of platform services that constitute the Broker.

Every device participating in the Swarm has a Broker installed in it. Since the Swarm network is composed of heterogeneous devices, the Broker number of platform services varies in the devices, according to their capabilities. Less powerful devices will provide fewer platform services. Accordingly, devices with minimum computing capabilities that do not allow installing new software have an external software *proxy* to translate communication.

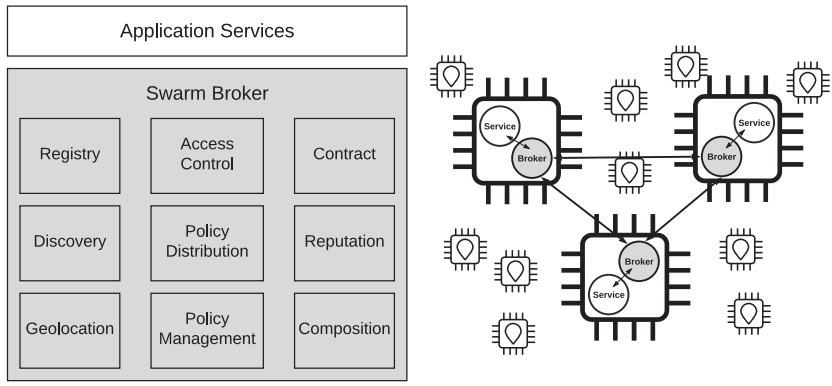

Figure 7.6 The Swarm OS broker organization.

Different implementations of the Broker are expected, to cover a wider range of devices. Currently, we have four implementations, using different programming languages: C, Lua, Java, and Elixir.

7.5.2.3 Semantic discovery in the Swarm network

Finding a suitable service to interact in the Swarm is a problem of major importance. The Swarm architecture, shown in Figure 7.7 proposes a functionality-based search of services. A requester service searches for a service that matches the expected functionality. Initially, an exact functionality-matching was implemented, based on string comparison, which poses severe limitations, such as not being capable of matching equivalent functionalities that use different names.

Several initiatives were devoted to exploring the use of semantics to the problem of service discovery. More recent work highlighted the opportunity

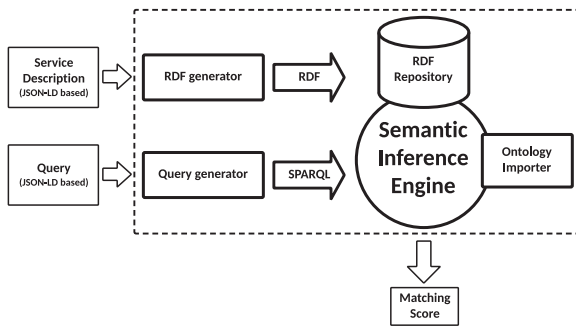

Figure 7.7 Architecture of the semantic registry service in the Swarm.

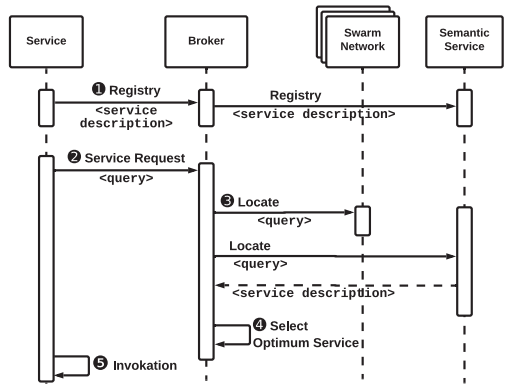

Figure 7.8 The semantic discovery process in the Swarm.

of applying those technologies to the Internet of Things. We here introduce a framework to enable semantic discovery of services in the Swarm, as shown in Figure 7.8. We describe the benefits of semantics for the aforementioned problems and present an architecture and implementation for our solution.

The authors in [6] propose a novel architecture for semantic discovery in a decentralized and heterogeneous environment, and a novel document format for service description and service request, focused on human friendliness and ease to use.

7.5.2.4 The Swarm economy

The distributed and decentralized nature of the Swarm network poses new challenges to security and transaction models. Traditional technologies, such as the public key infrastructure (PKI), are not suitable since they require a centralized certificate authority (CA). To overcome this challenge, the Swarm adopted the blockchain technology, used in the Bitcoin cryptocurrency, to create a decentralized mechanism for trust in the economic model of the Swarm network [7].

The economic model of the Swarm aims to regulate the transactions of services in the Swarm network. This model includes trust, a rewarding mechanism, billing, reputation, and a full virtual economy system. The model based on microeconomic principles applied to IoT services, has the following components: a *transaction* is a trade of *computing resources* between a *customer* and a *provider* of different *owners*.

The Swarm Broker is responsible for linking the parties and for facilitating transactions. The price of a resource is the number of credits necessary

for the service provider to grant access to the service consumer. Credits are the owner's asset; they are used by the service to contract or to purchase any service on behalf of its owner.

The Swarm economic model is based on the price of a service and on the reputation of both service consumer and provider; hence, it is called *price-reputation* model. A service provider defines the number of credits necessary to allow a third party to use it. On a service request, candidate providers are ranked by the lowest price according to the formula:

$$P = \begin{cases} P_{\min} + \frac{P_{\max} - P_{\min}}{T_{\text{th}}}(T_{\text{th}} - T_{\text{pc}}), & T_{\text{pc}} < T_{\text{th}} \\ P_{\min}, & T_{\text{pc}} \geq T_{\text{th}}. \end{cases}$$

During the transaction process, reputation points evaluate the success of the operation. The price-reputation transaction is the simplest transaction defined for the Swarm framework: the consumer gets the service by paying a number of credits settled by the provider, depending on their behavior, they both get reputation points during the process.

As the Swarm is an organic network of heterogeneous participants, a fair set of rules is necessary to guarantee a fair trading of resources. We created an economic model, following principles from microeconomics, as previous efforts did. We identified the participants of the model, created a taxonomy and proposed a microeconomic model for resource trading in the Swarm. The economic model describes how transactions take place in a distributed environment. The implementation of the price-reputation model takes advantage of the blockchain technology to store information credits and reputation of the participant devices.

The advances in an economic model for the Internet of Things go in the same direction of a growing trend in world economy called sharing economy. As in the physical world, the Swarm favors the digital sharing of resources over the acquisition of dedicated devices. As a consequence, it produces a reduction of device consumption and a better global use of resources.

7.5.2.5 Security and access control in the Swarm

The resource-sharing vision of the Swarm can only be implemented if security is built into the system. This includes both the use of appropriate algorithms and protocols to protect exchanged messages, and a flexible access control mechanism to govern which interactions are allowed. For example, the owner of a street-facing security camera may make it available for sharing during daylight, and a smart building will need different policies to control access to different devices on different floors, which are rented to different

stakeholders. Thus, managing the access among large quantities of devices becomes a significant challenge.

The Swarm approach to access control uses Attribute-Based Access Control (ABAC), a flexible and comprehensive system in which subject requests to perform operations on objects are "granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies specified in terms of those attributes and conditions" [8]. As ABAC is still in its maturation phase, a new model called ABAC-them was introduced. It focuses on combining simplicity and expressiveness, and its main characteristics are:

- Enumerated policies: attribute enumeration allows creating policies that are easy to parse and to embed into small devices.
- Hierarchical attributes: allow creating high-level policies that are easier to write and to understand. During execution time, low-level attributes present in access requests benefit from attribute hierarchies, which allow them to match with the high-level policies.
- Typed attributes: provides a counterbalance to policies that can grow large when using enumeration, such as those involving numerical ranges. Multiple attributes: very specifically, this feature allows easily creating conjunctions when using enumerated policies.

As an example, Figure 7.9 shows a policy written according to the ABAC-them model. It states that "any security appliance can be accessed and modified by an adult family member" and is serialized using Javascript Object Notation (JSON).

The ABAC-them model was implemented within an architecture based on the NIST recommendation for ABAC systems [8]. It comprises four main

```
{
  "user_attrs": [
    ["string", "Role", "AdultFamilyMember"]
  ],
  "operations": ["read", "update"],
  "object_attrs": [
    ["string", "Type", "SecurityAppliance"]
  ],
  "context_attrs": [
    ["time_interval", "DateTime", "* * 8-18 * * *"]
  ]
}
```

Figure 7.9 An access control policy example.

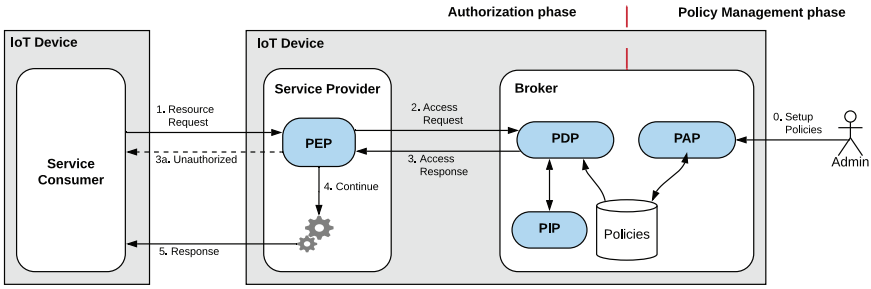

Figure 7.10 Security and access control architecture on the Swarm using ABAC policies.

points. The Policy Decision Point (PDP) evaluates policies managed through the Policy Administration Point (PAP), while the Policy Information Point (PIP) accounts for gathering context and other attributes, and the Policy Enforcement Point (PEP) intercepts requests and verifies their permission with the PDP. While the original NIST architecture proposes that the PDP, PIP, and PAP reside in an authorization server, the proposal within the Swarm puts all points inside the IoT device, thus enhancing its autonomy and security. One challenge emerging from this modification is that the policies are now distributed, and a policy-sharing mechanism must be developed. In a previous work, a policy distribution algorithm was implemented, which allowed devices to gather policies from surrounding devices, which would be edited by a human user, and then pushed the policies to the appropriate devices again [16]. Figure 7.10 shows the architecture of the access control module.

7.5.2.6 Resource-constrained devices: The Swarm minimum broker

The Swarm Broker is the software agent installed in each device to mediate the interaction with the emergent and complex network of devices. The Swarm Broker turns the device into a *swarm-insect*, i.e., a member of the Swarm. To overcome the challenge of heterogeneity in the IoT, particularly the integration of resource-constrained devices, a Minimum Broker (MB) has been proposed [9], which contains the core features necessary for a device to be part of the Swarm. Figure 7.11 depicts the interaction between Minimum Broker and common Swarm Broker, focusing on the discovery process.

The simplest possible behavior of a Swarm participant is to be able to be discovered and to provide information, as a simple sensor does. It is not hence necessary to support the creation of new locate requests, and only a simplified

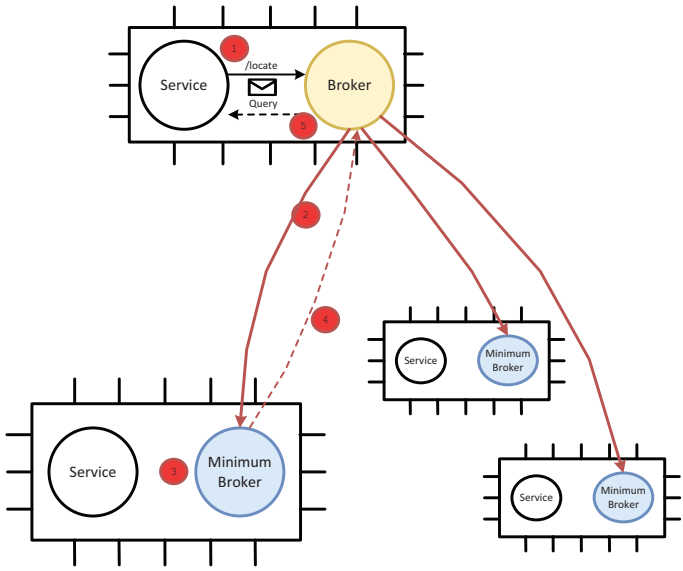

Figure 7.11 The discovery process in the Swarm minimum broker.

implementation for answering locate requests suffices. While the complete process for responding to location requests considers queries that arrive via either unicast (e.g. HTTP) or multicast (e.g. SSDP) and supports forwarding queries, the locate service in the MB only supports queries arriving via multicast. The reception of unicast locate messages was not considered an essential feature, as it is superseded by multicast in local networks, and would only work with the pre-requisite that a remote broker already knows the address of the Minimum Broker.

7.5.2.7 The future of platforms for the Internet of Things

In [10], G. Rzevski foresees the IoT as a complex network of devices, characterized by the seven properties of a complex system. *Connectivity*, with heterogeneous devices richly interconnected in a global network; *autonomy* of behavior, as edge devices become more intelligent; *emergent behavior* that results from device interaction; *nonequilibrium*, a common characteristic from markets is applicable to the future IoT when an economic model for resource trading is widely adopted; relations between participants are *non-linear*; thus, a small input can result in a large event (butterfly effect); *self-organization* is the ability to change the behavior or structure to adapt

to unexpected events; *co-evolution* states that as the IoT network changes, its environment also changes in an inevitable and irreversible way.

The characteristics above describe a common scenario that platforms for the future IoT should consider. As devices become more capable, richer interactions lead to the need of an adaptable, self-organizing platform for device cooperation. The common cloud-centric architecture of most IoT applications will be superseded by decentralized and distributed platforms, where edge devices will have a greater protagonist. Interaction models based on multi-agent systems will be the basis for the future IoT. The SwarmOS constitutes a step in this direction.

7.6 Regulation, Security and Privacy

The regulatory field in Brazil has been mainly affected by the actions of the National Agency of Telecommunications (ANATEL), and the LGPD. While Anatel is working towards reducing barriers to IoT large-scale adoption, the LGPD paves the legislative ground to protect the privacy of customers in all economic sectors, including the IoT.

7.6.1 Telecommunication Regulation

Anatel, an independent organization that has regulated and supervised telecommunication services in Brazil since 1997, is working towards the flexibilization and reduction of barriers to the expansion of IoT and M2M applications. In August 2018, and then again in August 2019, Anatel released a public consultation to receive inputs from society for 45 days, which are to be considered during the creation of new regulatory policies for IoT in Brazil [11]. These policies are expected to make the exploration of telecommunication services more flexible, facilitate the setup of roaming, and provide consumers with easy access to details regarding the service level they have contracted. The new regulation is expected to be approved by the end of 2020, and it is aligned with the IoT National Plan, which seeks to implement and push forward the IoT in Brazil.

A topic discussed recently within the agency is whether a specific service type for IoT applications should be created by the agency, with the ultimate decision being that it should not [12]. The main reason is that Anatel considers that the existing regulations for radiofrequency and telecommunications already allow a vast range of applications, and it would be easier to perform small changes to existing rules than to create a completely new regulation.

7.6.2 General Law of Data Protection

The use of IoT solutions that collect data in large scale raises concerns about privacy. Aligned with global concerns over the topic, such as the European General Data Protection Regulation (GDPR), the Brazilian Congress passed the General Law of Data Protection (LGPD), whose main goal is to enhance the privacy of personal data and to allow greater control over it from a consumer perspective. It also creates clear rules for how data should be treated by organizations and strengthens the power of regulatory agencies to perform control [PR2018]. According to a comparative analysis, the differences between LGPD and GDPR are minor, and the LGPD can be referred to as a "GDPR à la Brasileira" [13].

Approved in August 2018, the actual law enforcement is predicted to begin only on February 2020, so as to give companies an 18-month interval to adjust to the new regulation. The LGPD concerns all economy sectors and applies to every company that collects data in Brazil, independently of its source country. Therefore, every IoT company with operations in Brazil will need to comply with it. The law also provides that companies can only collect personal data with the consent of the users, which can request access to their data and demand its complete erasure at any time. Violations of the law may entail warnings, fines, and even partial or full suspension of operations, depending on the severity of the case. Regarding fines, the values may vary from 2% of the past year revenue to R$ 50 million, with the addition of daily penalties [14, 17].

7.7 Conclusions

The Brazilian National Plan for the Internet of Things helped to formalize and to converge ongoing IoT initiatives and to promote new ones. In this work, we summarized some selected work towards the accomplishment of the premises settled by the National Plan. Those initiatives were carried out by the University of São Paulo, the National Telecommunication Agency (Anatel), and the Brazilian Government comprehending strategic areas. The Code IoT education platform constitutes an investment in human capital, which has a direct impact on future technical developments. The Caninos Loucos Single Board Computer family and the SwarmOS IoT platform together constitute a national software and hardware platform for IoT. The five applications: Smart traffic lights, Smart surveillance, health monitoring of childhood cancer patients, sleep apnea diagnosis, and Internet of Turtles,

are representative examples of innovative application for smart cities, health and environment domains. Finally, the flexibilization of regulations by Anatel and the creation of the General Law of Data Protection (LGPD) constitute the advances in regulation, security and privacy.

The examples above constitute concrete efforts towards an extensive adoption of IoT technology in strategic areas. Although all these use cases have substantial results, their development continues as there is a clear demand for further advances.

Acknowledgements

The content of this chapter summarizes the work of different projects, coordinated by Brazilian institutions, such as the Centro Interdisciplinar de Tecnologias Interativas (CITI) from the University of São Paulo, and LSI-TEC.

Also, a number of institutions provided financial support for developing these projects, such as SMART Modular Technologies[6], the Ministry of Science, Technology, Innovation and Communications of Brazil (MCTIC)[7], the Brazilian Development Bank (BNDES), the Coordination for the Improvement of Higher Education Personnel (CAPES)[8], the National Council for Scientific and Technological Development (CNPq)[9], the University of São Paulo (USP)[10], Samsung[11], LG Electronics[12], and Santander Bank[13].

Further acknowledgements include:

- Caninos Loucos: Mr. August R. Machado, Mr. Tadeu M. Frutuoso, Eng. Sílvio Dutra, Dr. Casimiro de A. Barreto, Eng. Edgar Righi, Eng. Marcelo Ordonez, Eng. Guilherme Garcia, Eng. Sérgio de Paula, Mr. Mário Nagamura. Special thanks to Jon 'Maddog' Hall for his contribution and inspiration to the project, including the project name (*Caninos loucos* means *mad dogs* in Portuguese).

[6] https://www.smartm.com

[7] http://www.brazil.gov.br/government/ministers/science-technology-innovation-and-communications

[8] http://www.capes.gov.br/

[9] http://www.cnpq.br/

[10] http://www.usp.br

[11] https://www.samsung.com/us/

[12] https://www.lg.com/br

[13] https://www.santander.com.br/

- SwarmOS: Mr. Gabriel M. Duarte, Mr. Phillipe S. Rangel, Mr. Guilherme C. Marques, Mr. Gustavo Rubo, Mr. Carlos E. Laschi, Mr. Matheus B. Guinezi, Mr. Renan Oliveira, Mr. Douglas Navarro, Mr. Rafael C. Sales, Mr. John Esquiagola, Dr. Flávio S. C. da Silva.
- CodeIoT: Dr. Ana G. D. Correa, Dr. Marcelo A. José, Eng. Alexandre A. Martinazzo, Eng. Cassia Fernandez, Eng. Isabela Angelo, Eng. Leandro Coletto Biazon, Ms. Elena Saggio, Mr. Erich P. Lotto, Mr. Fábio G. Durand, Mr. Mário Nagamura, Mr. Rodrigo Suigh, Ms. Letícia Lopes, Mr. Renatto O. M. Domingues, Mr. Charles R. Silva, Ms. Julian Lepick, Sra. Lídia Chaib, Mr. Yohan Takai, Sra. Ohanna J. do Amaral, Mr. Migyael G. T. Vieira.

References

[1] Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). "Decreto que institui o Plano Nacional de Internet das Coisas é publicado". online at: https://www.mctic.gov.br/mctic/opencms/salaImprensa/noticias/arquivos/2019/06/Decreto_que_institui_o_Plano_Nacional_de_Internet_das_Coisas_e_publicado.html

[2] J. M. Rabaey, "The swarm at the edge of the cloud-a new perspective on wireless."2011 Symposium on VLSI Circuits-Digest of Technical Papers. IEEE, 2011.

[3] E. A. Lee, et al. "The swarm at the edge of the cloud." IEEE Design & Test 31.3, 2014, pp. 8–20.

[4] L. Costa, et al. "Swarm os control plane: an architecture proposal for heterogeneous and organic networks." *IEEE Transactions on Consumer Electronics* 61.4, 2015, pp. 454–462.

[5] J. Lewis and M. Fowler. "Microservices." *martinfowler. Com*, 2014.

[6] P. C. Calcina-Ccori, et al. "Enabling Semantic Discovery in the Swarm." IEEE Transactions on Consumer Electronics 65.1, 2018, pp. 57–63.

[7] L. De Biase, et al. "Swarm economy: a model for transactions in a distributed and organic IoT platform." *IEEE Internet of Things Journal,* 2018.

[8] V. C. Hu, et al. "Guide to attribute-based access control (ABAC) definition and considerations (draft)." *NIST special publication* 800.162, 2013.

[9] L. De Biase, et al. “Swarm Minimum Broker: an approach to deal with the Internet of Things heterogeneity.” 2018 Global Internet of Things Summit (GIoTS). IEEE, 2018.
[10] G. Rzevski and P. Skobelev. “Managing complexity”. Wit Press, 2014.
[11] Agência Nacional de Telecomunicações (ANATEL). “ANATEL aprova consulta pública para diminuir barreiras à expansão de IoT e M2M no Brasil”. online at: https://www.anatel.gov.br/institucional/noticias-destaque/2333-anatel-aprova-consulta-publica-para-diminuir-barreiras-a-expansao-de-iot-e-m2m-no-brasil
[12] Agência Nacional de Telecomunicações (ANATEL). “CONSULTA PÚBLICA N° 39”, online at: https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C2268
[13] C. Perrone and S. Strassburger. “Privacy and Data Protection-From Europe to Brazil.” *Panorama of Brazilian Law* 6.9-10, 2018, pp. 82–100.
[14] G. Camargo. “LGPD: 10 pontos para entender a nova lei de proteção de dados no Brasil” Computerworld, online at: https://computerworld.com.br/2018/09/19/lgpd-10-pontos-para-entender-a-nova-lei-de-protecao-de-dados-no-brasil/
[15] L. De Biase, et al. “Swarm Minimum Broker: an approach to deal with the Internet of Things heterogeneity.” *2018 Global Internet of Things Summit (GIoTS)*, IEEE, 2018.
[16] G. Fedrecheski, et al. “Attribute-Based Access Control for the Swarm with Distributed Policy Management.” *IEEE Transactions on Consumer Electronics* 65.1, 2019, pp. 90–98.
[17] Presidência da República. “Lei Geral de Proteção de Dados Pessoais (LGPD)”, online at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
[18] L. De Biase, et al. “Swarm economy: a model for transactions in a distributed and organic IoT platform.” IEEE Internet of Things Journal, 2018.
[19] F. Marques. “Brazil’s Internet of Things”. Pesquisa FAPESP, 259, 2017.