New Era of Mobile Access Control System

Gean Davis Breda, Raul Mariano Cardoso, Felipe André Cordeiro Pirotta

Dept. of Electronics and ComputingAddvance Technology – Unicamp (University of Campinas) Campinas, São Paulo - Brazil

Abstract
In the last century, due to the constant evolution of technologies, telecommunications networks have become increasingly robust, being able to support multiple services. Smartphones are increasingly incorporating these features and have become indispensable devices in our daily lives. This project is about the development of an autonomous access control system based on the use of smartphones as digital access keys. To do this we will follow the proposed methodology by the IoT-A (Internet of Things Architecture) to obtain an architecture of reference. The system consists of three main components: Web, Embedded and Mobile Application. This system allows the monitoring and remote control of actuators (Embedded Applications), for the opening and closing of doors or electronic gates through a mobile application, in a social manner and integrated with other services in the web (Web Application). The objective is to have a distributed system of embedded devices that connect to a centralized application in the cloud

Index Terms
Smartphones, Mobile, Network Communications, Internet of Things, Mobile Access Control System, Bluetooth, NFC (Near Field Communication).

1. Introduction

The fast Internet growth in the last fifteen years has triggered a paradigm change in our lives. The Internet is changing the way people around the world interact through technology, placing the end user at the center of every digital experience. At the same time, digital devices are enabling a new services. Today, the smartphone is becoming an indispensable tool in our daily lives. Since these devices have connection to the Internet, more and more services are offered through them, there are no longer limits in their use.

Moreover, the Internet of Things (IoT) is becoming a force capable of changing the way we interact, bringing each object, and consumer activity to the digital world. This is a highly innovative environment able to create new paradigms. The physical objects are becoming digital, they are becoming smart and connected to the Global Network Communication. They are no longer tight, you can now interact with them, or rather the objects begin to interact among them.

Most of the researches we have gone through was useful to show us that a new generation of access control demands necessarily the utilization of smartphones [1] associated with a biometric mechanism of authentication. This increases the probability that the person who presents the credentials is the real owner of it, to whom the access was initially released [2]. We can understand that, once the credentials are pieces of information that people either know (user/password) or have (RFID card). On the other hand, the utilization of smart phones associated with biometric patterns is information that people are (digital, face, iris). In this article, we will not delve into details regarding biometry. Different from the utilization of traditional keys which is around 2000 years old, the utilization of smartphones with digital keys, besides making the system safer and versatile/agile, it decreases the probability of error in the release of the access. Within this line of research, we are proposing an autonomous control system of access capable of managing the access of people to restrict environments by using smartphones associated with a Web solution that takes the Internet as a mean of communication and storage of information.

The proposed access control system is composed of three main components: Mobile, Embedded and Web Application. The whole system was modeled using concepts of IoT, more specifically the methodology proposed by the IoT-A [3]. As mentioned before, the system is distributed and composed by three distinct software/hardware, connected between themselves, working in synchrony offering services to the users, Figure 1. By definition it is a distributed system, composed of ‘things’, therefore a system aimed at IoT. To develop a set of scalable software with the following characteristics, capable of maintaining local databases and synchronized bases with network services, it is important to ground the choice in a architecture of reference that establishes macro forms and adequate patterns for implementation [3]. The project proposes the creation of a prototype for testing two cases: residential and vehicle access control.

The Web Application is the central element of the system, it is responsible for the coordination of all ‘high level’ applications. It receives, processes and transmits all the requirements and information for the Mobile and Embedded Application. This application controls the central database. The Mobile Application is the main interface for the user. Through this the user can register and schedule events in the desired access points (place). Through this application it is possible to, for instance, instantly open from a distance a determined place. And also through this application where

Manuscript received August 5, 2015
Manuscript revised August 20, 2015

the mobile phone transforms itself into a 'virtual key'. This 'virtual key' is transmitted through the Bluetooth Low Energy communication protocol (IEEE 802.15.4) [4] and NFC [5] to the reading module of the Embedded Application which controls the door/turnstile/gate.

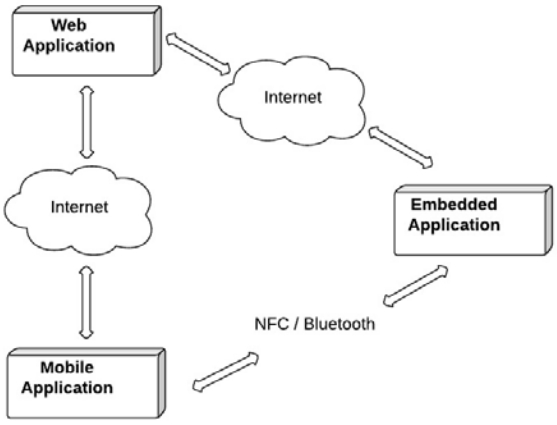

Fig. 1. System Design

The Embedded Application is the element responsible for controlling the access point, it generally has a reading and an actuator module. The reading module is responsible for establishing a communication channel with the smartphone (Mobile Application), for it uses two technologies, NFC and Bluetooth. Through these channels the information, virtual key, is passed to the Embedded Application. The actuator module is responsible for physically operating in the door/turnstile, etc., allowing or not the access. The Embedded Application maintains a constant communication with the Web Application, where it receives, among others, the information which refers to the users who are able to enter the place, as well as, send information related to the events (logs) that are happening. The Embedded Application has, for example, a copy of the central database, but only the relevant information that is related to the access point (place). This is a contigency action for moments when there is a communication failure. Therefore the application has a certain autonomy which enables an action even when there are communication problems.

2. IoT-A METHODOLOGY

The methodology proposed by the IoT-A is recent, as well as the Internet of Things. We have seen an increasing use of both the modeling as well as the concepts related to IoT . We have found various projects that work with these concepts. The project developed by Kelly & Mukhophyay [6] proposes the use of IoT to monitor domestic environment by using a low cost ubiquitous sensor network. In this sense, architecture, interconnecting mechanisms and security are created so that they can guarantee the functionality of the system. In the work of YUN & Yuxin [7] the authors raise the difficulty of making numerous heterogeneous system components talk to each other. In this sense the researchers propose the use of the IoT Architecture. Already in Zhu, Wang, Chen, & Liu [8] the authors propose the creation of a IoT gateway based in the ZigBee and GPRS protocols. Therefore various requirements have been researched for the system.

The first great IoT contribution is the IOT-Architectural Reference Model – ARM. The Reference Model provides concepts and definitions on which the architecture can be built [9]. The Reference Model consists of various submodels. The main one that serves as a starting point for the elaboration of them all is the Domain Model. It describes the concepts that are relevant to the Internet of Things. All other submodels and even the Reference of Architecture are based on the concepts presented in it [10].

From the Domain Model, the reference laid by the IoT-A Project determines that an Information Model should be developed, which represents the information that are manipulated by the Internet of Things system. The third model is the Functional Model. This model identifies groups of functions concerning the Domain Model concepts. A functional group provides the functionality for interacting with instances of the Domain Model concepts. Another component that must be addressed is the communication between different components. Thus, the Communication Model introduces the concepts which permit the communication representation in the Internet of Things environment. The Iot-A also proposes a Security Model that represents the related aspects to the system which is being scaled.

3. Architecture Designed Following The IoT-A METHODOLOGY

Below we present/describe the models that make up the proposed architecture.

3.1. Domain Model

The main aim of the Domain Model is to create a common understanding of the project in itself, main concepts and relationships. Only with a common understanding is it possible to discuss architectural solutions and evaluate them. The model does not address private technologies, but its abstractions. An IoT scene can be described, in a generic way, as a user wanting to interact with a Physical Entity in the real world.

The domain model is composed of various elements, among them [3][9]:

- Physical Entity – Represent the physical elements of the system that is part of the modeling. Physical Entity can be any physical component from the real world;
- Virtual Entity – All Physical Entities have a virtual representation, this is done through Virtual Entities. Virtual Entities are representations from a series of aspects or properties of the Physical Entities.
- Device – devices provide an interface between the digital and physical world, that is, a link between the virtual and physical entities. Usually we can have the following devices, among others:
    - Actuators- are able to modify the physical state of a Physical Entity, as changing the state, i.e: they work by physically opening doors/gates;
    - Sensors – Provide information, data from the Physical Entity ;
    - Tags – Are used to identify the Physical Entities, which are generally fastened. The identification procedure is done through reading;
- On Device Resource – They are software components which provide information about a Physical Entity or enable the performance over it;
- Active Digital Artefact - They are software components which access other services or resources from the System. Run components, applications, agents, services that can access other services or resources;
- Service – A service provides a well defined/standardized interface that provides all functionality needed for the interaction of a Physical Entity and procedures that are related.

Figure 2 introduces the Domain Model. The following will detail some functions of the main components of the domain model. The Physical Entity "Owner Device" is associated to its correspondent Virtual Entity, it concerns the person who will use the system. The Physical Entity has the "IoT phone", that is a smartphone that have NFC/Bluetooth interface communication to transmit Tags (Ids). Also in the cellphones we have the "App Android" which is responsible for providing the user interface with the system. The application is able to execute various functions direct and indirectly in relation to the Web and Embedded Application, they are:

- "Login" – Access the system through a user and a password;
- "Open Door WebApp" - It allows an actuator to be activated from a distance (Remote opening), i.e, the opening of a door;
- "Phone" – Updates the data related to phones. It associates the telephone which the user logged in to, so that this can be used to access restricted areas;
- "User Register" - It enables the user to authorize individuals to access restricted areas.

The majority of the functions mentioned above also can be executed through a computer (with an internet connection), through an access to a "Front End" (Interface) of the Web Application, besides the following functions:

- "Devices Register" – it enables new devices, module readers/actuators, to be registered in the system. We use the word "devices" to represent devices;
- "Groups Register" – it enables new groups to be created in the system.

The Web Application also has a central database which concentrates the information of the system. The "Update module" service, as the name says, is responsible for updating the information related to the devices, dates/appointments, in the respective local database of the Embedded Applications. The second function of this service is to record the logs generated in the Embedded Application in the central database. The Embedded Application has a Physical Entity which is designated by the Access Point and its correspondent Virtual Entity. Connected to the Access Point there is a device called "Control Module" which has an actuator and NFC/Bluetooth reader. The readers are responsible for capturing the "digital keys", that is, transmitted information by the smartphones as soon as they approach the device. These information are stored and simultaneously read by the "NFC/BT" service that transmits it to the service, the "Authorizer" responsible for verifying if the ID's are authorized to acess in the place in the specified time. If the ID is authorized the service called "Open Door" sends information to the actuator to liberate the access. This type of access is called local opening. Still in the Embedded Application there is a service called "Log" which is responsible for the creation of logs related to the events which happen in the control module, both in relation to the actuator as in relation to the readers. The logs are stored locally, "Log" (On Device Resource), later they are transmitted to the central database.

3.2. Information Model

The Physical Entities can create or receive relevant information for the system, information that can create actions or simply be stored in databases. The Information Model defines the structure of all information which is manipulated in the system in a conceptual level. This includes modeling of the main concepts for the information flow, storing and how they are related [9].

The Information Model details the modeling of a Virtual Entity, that is, it has a direct relationship with the Domain Model. This Virtual Entity has a name and type, and one or more values. The main aspects addressed by the modules are virtual entities, service descriptions and associations. A Virtual Entity models a Physical Entity and a service description describes a service that acts as a bridge to the physical world. Through an association a connection can be

modeled between an attribute of a Virtual Entity and describes a service. As mentioned above, the information present in the Information Model are always associated to the virtual entities, as well as determined services that manipulate them.

Figure 3 presents an Information Model for the Virtual Entity "User". The complete Information Model includes all the Virtual Entities. The associations in relation to the virtual entities are shown in the figure through solid lines. Now the relationship with services is shown through dotted lines.

3.3. Functional Model

The functional model is composed of seven longitudinal functional groups and two transversal ones. The transversal groups provide security and management for each longitudinal group. The policies that govern the transversal groups are not only applied to the groups themselves but also permeate the longitudinal groups. For instance, for the security policy to be effective, it must be ensured that no functionality of one component bypasses security in such a way as to permit unauthorized access [9].

A brief description of each functional group:

- Application – Represents an interface with the user of each presented module.

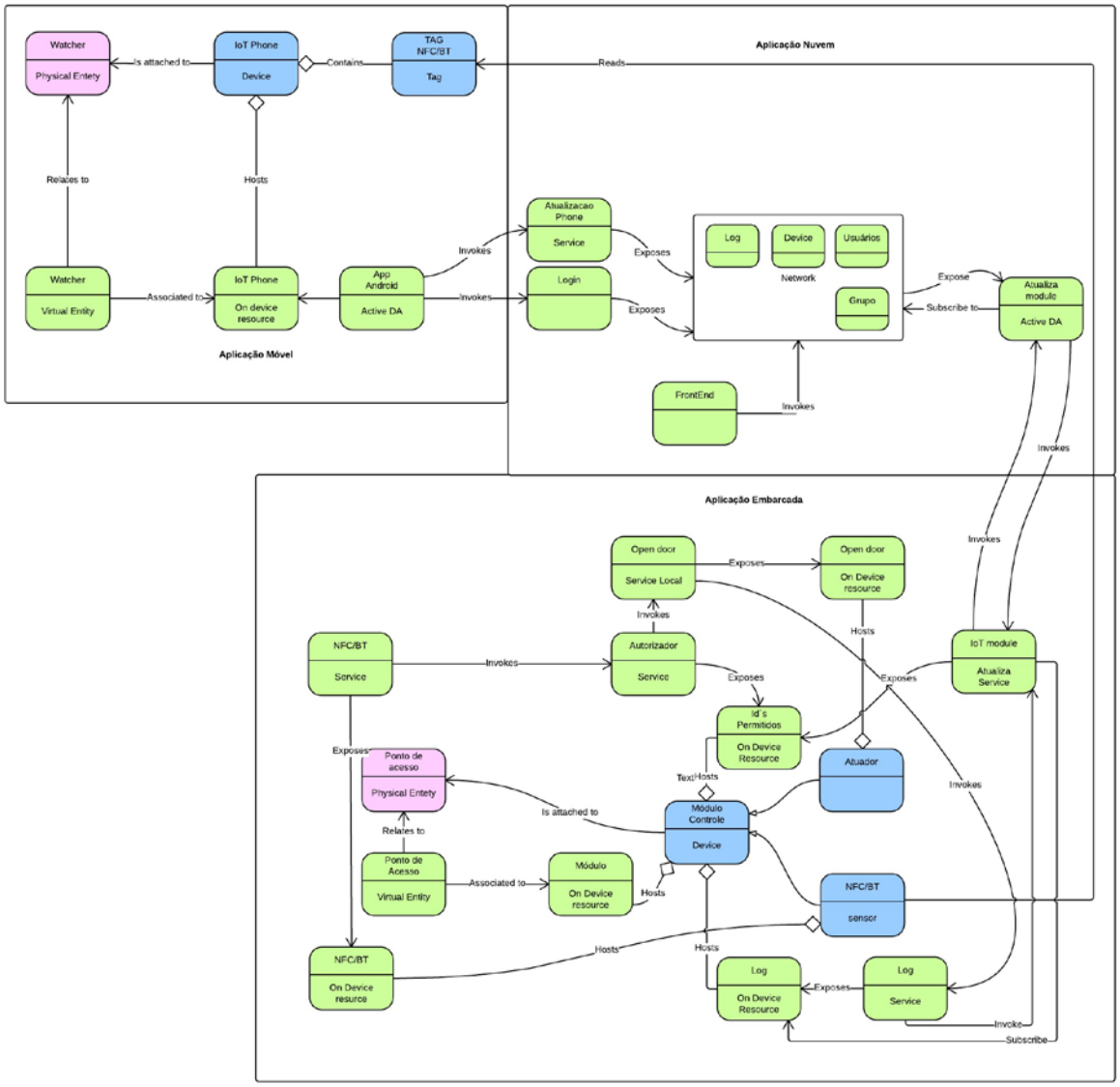

Fig. 2. Domain Model

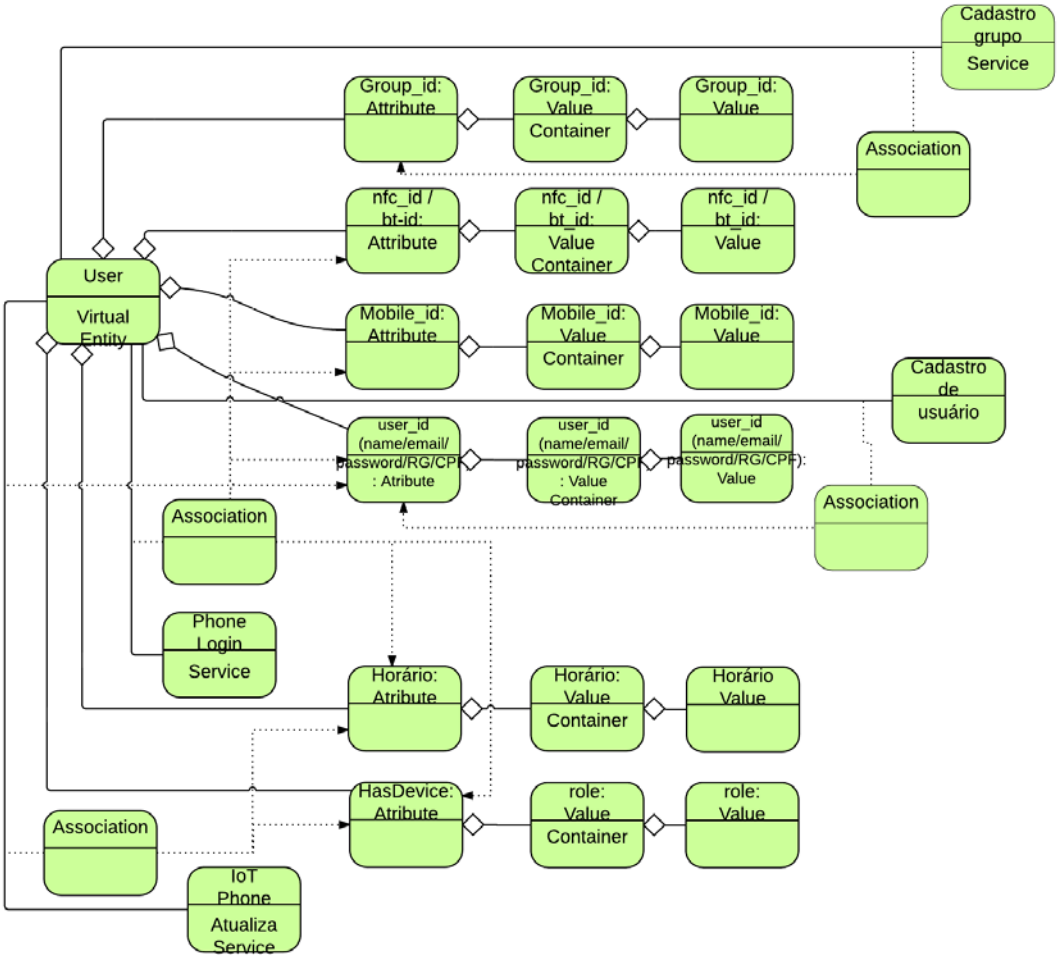

Fig. 3. Information Model

- IoT Process Management – is responsible for integrating traditional business to the projected system based on the IoT-A-ARM framework;
- Service Organization - it acts as a bridge to various other functional groups. This functional group is used to compose and arrange services of different concept levels;
- Virtual Entity – Good for modeling the Virtual Entity and consequently the Physical Entity;
- IoT Service – Contains services and functionalities of discovery, search and name resolutions for services aimed at IoT;
- Communication – Seeks to supply all communication system needs. This layer is responsible for ensuring interoperability between different types of networks;
- Management transversal – The objective behind management is: lower costs; meet the demand of users that were not anticipated; fault management and system flexibility.
- Security transversal – it is responsible for ensuring security and privacy of the system.

As to the items mentioned above, the most adequate Functional Model for the modeling of the proposed system does not contemplate the IoT Process Management and Service Organization component.

Figure 4 shows how the Functional Model was designed.

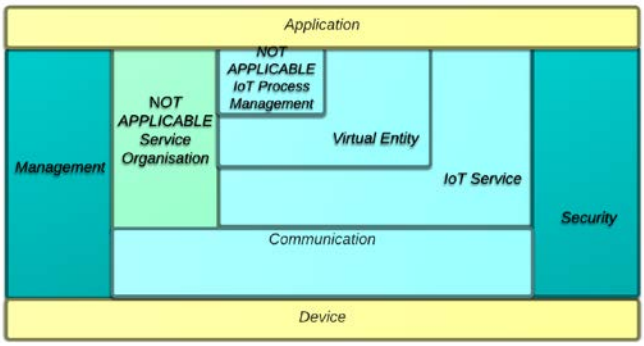

Fig. 4. Functional Model

3.4. Communication Model

This model shows the means of communication between the system agents. It devides the means of communication in "constrained network" (NTC) and "unconstrained network" (NTU). The first refers to a network with resource restriction, that is, transfer rate lower than 1 Mbps (Megabit per second) and high latency. Our system adopts the following wireless network that can be considered "constrained networks": Bluetooth and NFC.

The second, "unconstrained network", refers to different types of networks and network nodes with a significant processing capacity and availability, in our applications we can mention the 3G/4G networks, other internet networks (telecom providers), local networks as (Ethernet and WiFi). Figure 5 shows a sample of communication links and the correspondent technologies that can be used in our system. Here follows two of the seven designed communication models of the system.

Local Opening

Figure 6 is called local opening, the access procedure an individual executes, for example, at a business condominium. That is, a person with a registered smartphone approaches the turnstile/gate and from there the passing of information begins between the equipment and the Embedded Application to verify if the person has permission to enter.

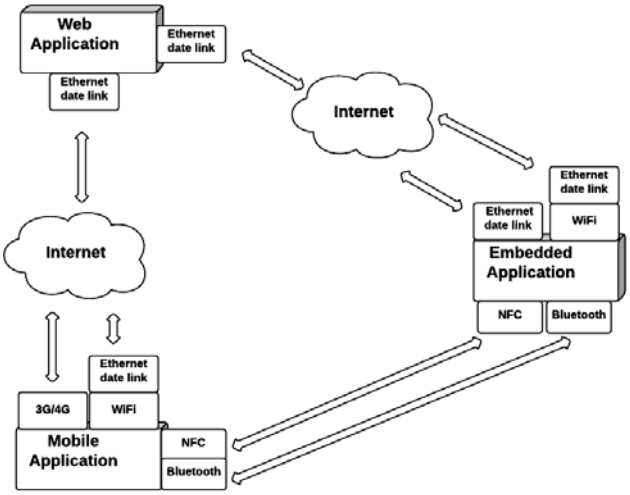

Fig. 5. Communication Links Model

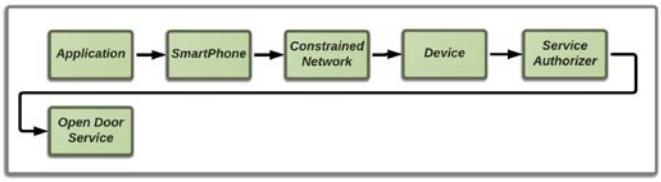

Fig. 6. Local Opening

Authorization

The authorization, Figure 7, is done every time a person enables another individual to enter the environment. The authorization involves sending information related to the event (date, time and place) of the person responsible and consequently the acceptance of the guest. All these information remain registered in the Central Database (Web Application) and later are sent to the Local Database (Embedded Application).

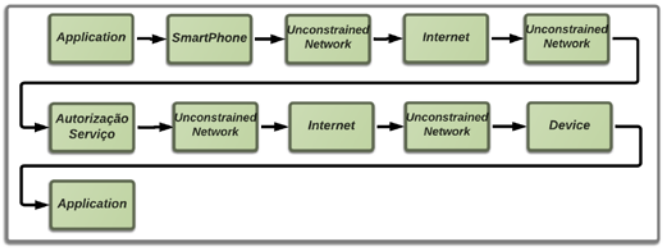

Fig. 7. Authorization

3.5. Security Model

The IoT system integrate objects, computational data and physical devices, in a transparent form, in a global network information about "intelligent things". In this picture, the services are like bridges through which these "intelligent things" integrate with the others in an automatic way with little or no human intervention. The aim is to supply an architectural reference for the Internet of Things system, therefore, it is obligatory to discuss potential security problems and to define the security model for our architecture [9].

This topic presents the main actions that were taken to guarantee the security of our system [11-14]: Encrypted communication channels; firewall in the Embedded and in Web Application; better methods in relation to login/passwords; device authentication; central system management; encrypted database.

4. SYSTEM

A seguir daremos alguns detalhes em relação ao desenvolvimento das aplicações Web, Embedded e Mobile,

4.1. Web Application

The Web Application has as its objective to be the integrator of the AirKey system. It is through it the administration and management of the system is done. This application is responsible for coordinating all "high level" applications. It receives, processes and transmits all the requisitions and information to the Mobile and Embedded Applications.

Some of the main functions of the Web Application are now listed:

- Automatic updating of the embedded devices
- User authorization and authentication
- Registration, exclusion and editing of users
- Registration of mobile devices
- Control of Central Database
- Storage of logs of the embedded devices
- Remote opening
- Creation and management of groups

The Web Application was developed in the Ruby language by using the framework MVC Ruby on Rails, presently hosted in the servers of AWS (Amazon Web Services).

The communication between this application and the other modules of the system is being carried out in two main ways. For the communication between the server (Web Application) and the Mobile Application we are using HTTPs requisitions once this bring us some flexibility of communication, and for the Embedded Application we are using WebSockets quite safely.

We are also concerned to the performance of the system keeping in mind that the application will have to bear an array of simultaneous connections through the WebSockets and HTTPs requisitions. The application was hosted in an environment able to dynamically allow replication and control of instances. In the tests carried out, the system has shown a stable behavior, no matter keeping the WebSockets connections with the devices or getting the answers via HTTPs and in the navigation through the platform.

4.2. Embedded Application

The Embedded Application is responsible for controlling the access of people to the environment, no matter either physically by means of barriers and/or turnstiles or by sending electronic notifications to the person in charge. People use their smartphones (Mobile Application) to identify themselves in the system. The digital key (MACaddress/IMEI) is passed from the smartphone to the Embedded Application through the Technologies of Bluetooth LE (Low Energy) or NFC (Near Field Communication).These technologies can be employed simultaneously in a same device, so offering flexibility to the kind of technology adopted.

The Embedded Application is responsible for doing the reading/capture of this identification (digital key) and, by checking the local database, release or not the entry, generating the due notifications/logs.

The nucleus of the Embedded Application is the control module board which runs an operating system of open code, a Linux distribution based on the OS (Operating System) Debian. The control module board is responsible for making the Embedded Application connect to Internet through WiFi, and with the Web Application through the NFC and Bluetooth.

The connection with Internet is necessary for the Embedded Application to be capable of communicating to the Web Application, having in mind that it contains all the pieces of information about the users of the system (Central Database). In a nutshell, the communication with the Web Application has three main goals: 1. Keep the Embedded Application up-to-date. This is done by updating a local databank with the pertinent information for that device. That is, which people are authorized to utilize the system at that point, in a given time, and which ways these users have to access, for instance, smartphones or RFID cards. 2. Enable the authorized user to control the system at distance. 3. Transmit log and notifications generated to the Web Application. These pieces of information are generated as a result of the accesses going on at that point.

4.3. Mobile Application

The Mobile Application is the main interface between the user and the system. Through this application it is possible; for example, to open a determined place at distance, instantly. It is also through this application that the cellular phone becomes a "digital key".

Next, we present the main functions of the Mobile Application:

- Authentication of users in the Web Application.
- Addition/removal of users to groups of access in the Web Application;
- Remote opening of embedded devices which the users have permission for;
- Communication through NFC or Bluetooth with the Embedded Application for the access control.

The Mobile Application was developed for the OS Android, from the 4.4 KitKat version.

The performance of the Mobile Application is according to expectations, as it is a light and simple application. We have carried out tests with compatible devices and we succeeded in installing/handling and utilizing the functions inherent to it.

The Mobile Application is being developed in JAVA, a programming language oriented to objects, competitive and based on classes, aiming to have the least possible implementation dependence. It was adopted as a base language for the apps developed to the Android platform.

One of the technologies utilized in the communication of the Mobile Application and the Embedded Application is the Bluetooth protocol. Initially, as previously mentioned, the communication was developed without any pairing, just using information from the Bluetooth MacAddress as the identifier, employed in the release of the access.

Another technology utilized as a mean of communication with the Embedded Application is the NFC. The cellular

device emulates internally a NFC card. The figure 8 explains better how this system works in the mobile device.

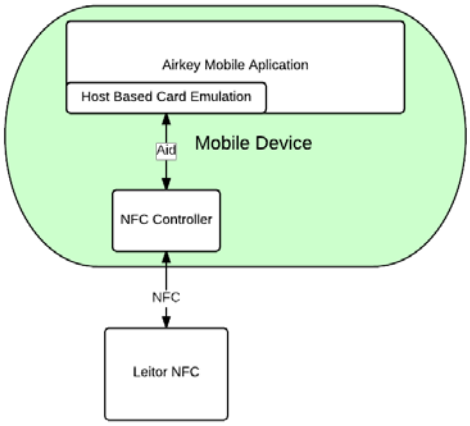

Fig. 8. NFC Model

The NFC reader coupled to the Embedded Application communicates with the Mobile Application through a request of connection with the HCE (Host Card Emulation), by using the standard AId (Application Identifier), after having established the initial connection between the reader and the mobile device. The Mobile Application, then, through a channel of communication with the reader send the information concerned the IMEI (International Mobile Station Equipment Identity) back to the device. In this case the IMEI is employed as an identifier in the control of access. This process is done in an active way by the Embedded Application and in a reactive way by the Mobile Application, that is, it just waits a requisition through the NFC Controller of the mobile device.

This possibility of emulating the Tags is only available from the Android 4.4 version. In the previous versions, it is not possible to do this kind of operation. In relation to the communication, the elements are configure as you can see in the figure.

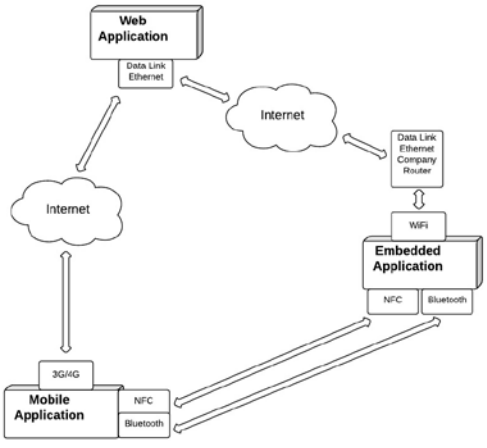

Fig. 9. Prototype Communication Links

The Embedded Application is connected with a LAN network (Local Area Network) available in the company named Advance through a connection WiFi 802.11 with a gross transference rate of approximately 54 Mbps.

The Web Application is hosted in a web service offered by Amazon Web Services (AWS), physically located in Sao Paulo, Brasil.

As for the smartphones used in the tests, they have the 3G/4G-type connection. In case of utilizing the 3G/4G technology, the appliances are connected to the Internet through their respective operators of telephony. The communication between the smartphones and the Embedded Application is done through the Bluetooth LE or NFC modules.

In Figure 10 and 11 it is possible to see the prototype solution components that were implanted (Embedded Application), it is possible to see the actuators (door/gate)

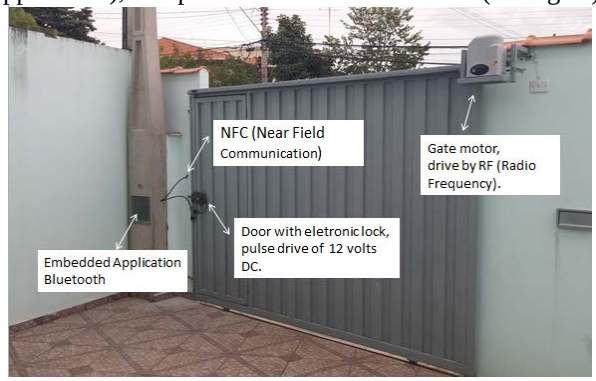

Fig. 10. Prototype embedded actuators and readers

Fig. 11. Prototype Embedded NFC Reader

In Figure 12 and 13 it is possible to see the prototype Embedded Application components. The Control Module is composed by the main board which controls the following peripheral modules: WiFi, Bluetooth; NFC; Ethernet. Besides, it has the control over the drive board which is responsible for altering the state of the actuators. The action at the door/gate is done through two outputs from the control module GPIO (General Purpose Input/Output).

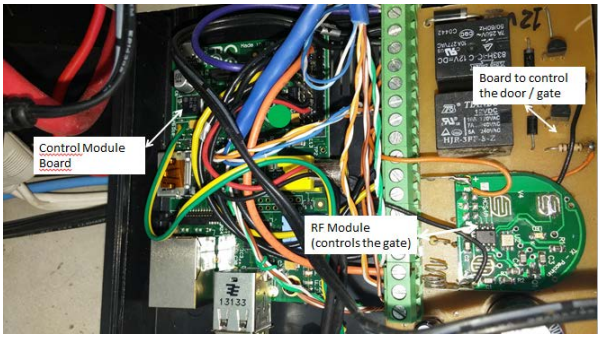

Fig. 12. Components of Embedded Application

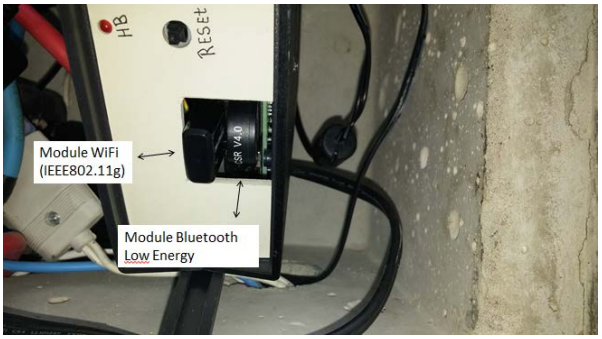

Fig. 13. Module WiFi and Bluetooth of Embedded Application

It is shown in Figure 14 the system performance between 18 and 27, May/2015. We show the opening of the door/gate using the Bluetooth and NFC technologies, as well as the remote opening.

The opening time of the door/gate, after putting the smartphone in the NFC reader is around 1 (one) second. The major problem related to the NFC lies in the size of the box in which the card (reader) is inserted. Due to the box being large and the reader having a narrow range of reading, there are positions (upper part/lower part) in which the reader can not establish any communication with the smartphone. However, in a normal range, the reading and activation is done quite quickly.

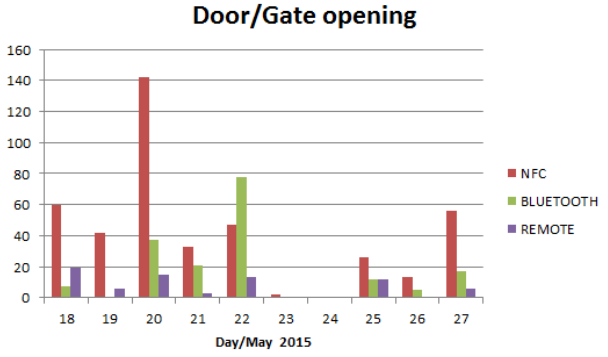

Fig. 14. Door/gate opening during 10 days in May/2015

As for the Bluetooth, as previously mentioned, we have some difficulty concerning the distance that the smartphone is read. We looked for lessening the distance to one meter, so that, not to activate the door/gate too often. The activation time is very similar to the NFC technology, that is around 1 (one) second. When driving, it is necessary to get close to the gate and position the cellular next to the windshield of the car.

In the following addresses some videos demonstrating these operations were published:

https://www.youtube.com/watch?v=WDNmQzO91lU
https://www.youtube.com/watch?v=-neyLzfVUdo
https://www.youtube.com/watch?v=Sh-MABGFlss
https://www.youtube.com/watch?v=ewYrRoyyos4

Concerning the performances of the Web, Embedded and Mobile Applications we can say they are within the expectations.

Conclusion

The adoption of recent technologies, for example the NFC, has demanded us to do some alterations both in hardware and software along the development of the project. We have changed the development platform of the Embedded Application to the module with operating system, aiming to have a development module with Operating System and available drivers. Another advantage of this migration is that it enables us, if necessary, to move easily to any platform based on Linux.

The initial plan for the Mobile Application was to utilize the concept of multiplatform (Cross Platform). However, and again, due to the specifications of the NFC and Bluetooth Low Energy, we ended up opting to work on the application of Android which owns about 80% of the Brazilian Market. The own modeling tool proposed by IoT-A proved a much broader way than we thought initially. It is a very effective method to model Internet of Things solutions. The architecture designed using the IoT-A methodology proved quite suitable to build the prototype.

As you can see in the course of this article, we have achieved the goals, we have succeeded in building this first architecture and prototype. We have functional solutions, built using the newest available technologies. The test showed that the system as a whole had stable behavior as it was used. We had a few problems in the beginning as soon as the module was installed, that were solved as the system was used. The central and local data bank showed a great performance even in situations with high/extreme load. The Mobile, Embedded and Web Application are trustworthy. Not only have we shown the feasibility of the system/architecture, as we have identified the points that if

exploited will be new competitive advantages in respect to what there is already.
Now, getting close to the end of the first part of the project, we are aware of new possibilities. Our interest is to give continuity to the improvement of the product by incorporating new functionalities.

Acknowledgment

This project have been supported by FAPESP (Fundação de Amparo a Pesquisa do Estado de São Paulo).

References

[1] Derawi, M. O. Biometric Access Control using Near Field Communication and Smart Phones. 2012 5th IAPR International Conference on Biometrics (ICB) (pp. 490-497). 2012,IEEE.
[2] Fenske, J.. Biometrics in new era of mobile access control. Biometric Technology Today , Vol. 2012, Issue 9, pp. 9-11.
[3] Magerkurth, C. (2013). Deliverable D1.4 - Converged architectural reference model for the IoT v2.0. Internet of Things - Architecture.
[4] Frantti, T., & Roning, J. (2014). A Risk-Driven Security Analysis for a Bluetooth Low Energy Based Microdata Ecosystem. Sixth International Conf on Ubiquitous and Future Networks (ICUFN), (pp. 69-74).
[5] Urien, P., & Kiennert, C. (2012). A New Keying System for RFID Lock Based on SSL. The 9th Annual IEEE Consumer Communications and Networking Conference -, (pp. 42-43).
[6] Kelly, S., & Mukhophyay, S. (13 de May de 2013). Towards the Implementation of IoT for Environmental Condition Monitoring in Homes. IEEE Sensors Journal (Volume:13 , Issue: 10), pp. 3846 - 3853 (Doi: 10.1109/JSEN.2013.2263379).
[7] Yun, M., & Yuxin, B. (2012). Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid. International Conference onAdvances in Energy Engineering (ICAEE), (pp. 69 - 72 (Doi: 10.1109/ICAEE.2010.5557611).
[8] Zhu, Q., Wang, R., Chen, Q., & Liu, Y. (2010). IOT Gateway: BridgingWireless Sensor Networks into Internet of Things. 2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC) (pp. 347 - 352). Hong Kong: IEEE.
[9] Bauer, M., & et all. . (15 de July de 2013). Internet of Things - Architecture. IoT-A Deliverable D1.5 - Final Architectural Reference model for the IoT V3.0, pp. 51 - 107.
[10] Walewski, J. W. (2012). Internet of Things Architeture IoT-A Deliverable D1.4 - Converged architectural reference model for IoT v2.0. Internet of Things Architectural, pp. Disponível em: < http://www.iot-a.eu/public/public-documents/documents-1 > Acesso em 05/05/2015.
[11] Holzer-Graf, S., & et all. (2013). Efficient Vector Implementations of AES-based Designs: A Case Study and New Implemenations. Topics in Cryptology – CT-RSA 2013 Lecture Notes in Computer Science, pp. 145–161.
[12] Kasper, E., & Schwabe, P. (16 de 06 de 2009). Faster and Timing-Attack Resistant AES-GCM. Cryptographic Hardware and Embedded Systems – CHES 2009 Lecture Notes in Computer Science , pp. 1-15.
[13] Narula, M. S., & Singh, S. (2014). Implementation of Triple Data Encryption Standard using Verilog. Int. Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X, 667-672.
[14] Xu, G., & Yu, B. (2011). Security Enhanced Design of the Bluetooth Simple Pairing Protocol. International Conference on Computer Science and Network Technology, (pp. 292-296).