ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

GRADO EN INGENIERÍA TELEMÁTICA

IMPROVING THE SECURITY OF IOT DEVICES BY IMPLEMENTING A LOCATION-BASED ACCESS CONTROL

Autor: Iciar Ortega Oria de Rueda
Director: Rafael Palacios Hielscher

Madrid

Junio 2018

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

Improving the security of IOT devices by implementing a location-based access control

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 2017/18 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido

tomada de otros documentos está debidamente referenciada.

Fdo.: Iciar Ortega Oria de Rueda Fecha: 11/07/2018

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Rafael Palacios

Fdo.: RAFAEL PALACIOS Fecha: ..11../ JUL/ 2018

AUTORIZACIÓN PARA LA DIGITALIZACIÓN, DEPÓSITO Y DIVULGACIÓN EN RED DE PROYECTOS FIN DE GRADO, FIN DE MÁSTER, TESINAS O MEMORIAS DE BACHILLERATO

1º. Declaración de la autoría y acreditación de la misma.

El autor D. Iciar Ortega Oria de Rueda DECLARA ser el titular de los derechos de propiedad intelectual de la obra: *Improving the security of IOT devices by implementing a location-based access control*, que ésta es una obra original, y que ostenta la condición de autor en el sentido que otorga la Ley de Propiedad Intelectual.

2º. Objeto y fines de la cesión.

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad, el autor **CEDE** a la Universidad Pontificia Comillas, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, los derechos de digitalización, de archivo, de reproducción, de distribución y de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual. El derecho de transformación se cede a los únicos efectos de lo dispuesto en la letra a) del apartado siguiente.

3º. Condiciones de la cesión y acceso

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia habilita para:

a) Transformarla con el fin de adaptarla a cualquier tecnología que permita incorporarla a internet y hacerla accesible; incorporar metadatos para realizar el registro de la obra e incorporar "marcas de agua" o cualquier otro sistema de seguridad o de protección.
b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.
c) Comunicarla, por defecto, a través de un archivo institucional abierto, accesible de modo libre y gratuito a través de internet.
d) Cualquier otra forma de acceso (restringido, embargado, cerrado) deberá solicitarse expresamente y obedecer a causas justificadas.
e) Asignar por defecto a estos trabajos una licencia Creative Commons.
f) Asignar por defecto a estos trabajos un HANDLE (URL *persistente)*.

4º. Derechos del autor.

El autor, en tanto que titular de una obra tiene derecho a:

a) Que la Universidad identifique claramente su nombre como autor de la misma
b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio.
c) Solicitar la retirada de la obra del repositorio por causa justificada.
d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

5º. Deberes del autor.

El autor se compromete a:

a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.
b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.
c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e

intereses a causa de la cesión.

d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción de derechos derivada de las obras objeto de la cesión.

6º. Fines y funcionamiento del Repositorio Institucional.

La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, y con fines de estudio, investigación, o cualquier otro fin lícito. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

- ➢ La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.
- ➢ La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusive del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.
- ➢ La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro.
- ➢ La Universidad se reserva la facultad de retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Madrid, a 11 de Junio de 2018

ACEPTA

Fdo……………………………………………

Motivos para solicitar el acceso restringido, cerrado o embargado del trabajo en el Repositorio Institucional:

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

GRADO EN INGENIERÍA TELEMÁTICA

IMPROVING THE SECURITY OF IOT DEVICES BY IMPLEMENTING A LOCATION-BASED ACCESS CONTROL

Autor: Iciar Ortega Oria de Rueda
Director: Rafael Palacios Hielscher

Madrid

Junio 2018

Agradecimientos

En primer lugar, quiero agradecer a mis padres el haberme apoyado siempre y el haberme animado a estudiar lo que me gustaba. Muchas gracias por haberme ofrecido la oportunidad de estudiar esta carrera y de hacerlo en el lugar que quería. Muchas gracias por siempre intentar ayudarme en todo lo que podíais. Sin vosotros no estaría aquí.

Muchas gracias a mi madre. Ella siempre ha sido y será mi principal apoyo. Me ha ayudado a lo largo de toda esta carrera, animándome y apoyándome cuando más lo necesitaba, en todos los malos tragos que he pasado estos años, pero también ha celebrado conmigo todas las metas que he conseguido ir superando. Sin ella no estaría aquí ahora mismo.

Gracias a mi padre, por quererme como lo hace, por siempre confiar en mi y en que puedo hacer lo que sea. Es esa confianza la que hace que yo haya tenido más confianza para lograr lo que me proponía.

Muchas gracias a mis hermanos. Para mi sois dos modelos a seguir, dos referentes que me animan a mejorar. Siempre he estado y estaré muy orgullosa de vosotros.

Quiero agradecérselo también a todos mis amigos, por hacerme pasar los momentos tan buenos que hemos pasado estos cuatro años; por todo lo que han hecho para que estos años sean tan especiales. Por haber sufrido conmigo y por haber disfrutado conmigo. ICAI puede llegar a ser muy duro, pero, gracias a ellos, no lo ha sido tanto. En especial quiero agradecérselo a Alex, la persona que más me ha cuidado, más me ha ayudado y más ha confiado en mi en los últimos años. Gracias por hacer estos años de carrera tan especiales y por estar ahí siempre que lo he necesitado.

Por último, quiero agradecerle este trabajo a mi director, Rafael Palacios. Estoy muy agradecida ya que, sin ti, no tendría trabajo hoy. Muchas gracias por haberme ayudado cuando estaba perdida en Boston sin saber que hacer. Gracias por haberme dado este gran proyecto y por haberme ayudado cada semana, dándome nuevas ideas y estando siempre muy atento. Ha sido un placer trabajar contigo. Siempre estaré muy agradecida.

Gracias a todas esas personas que, a lo largo de estos años, me han ayudado a aprender cosas nuevas y me enseñado lecciones muy valiosas para el futuro, entre ellos a mis profesores.

Muchas gracias por todo el apoyo.

IMPROVING THE SECURITY OF IOT DEVICES BY IMPLEMENTING A LOCATION-BASED ACCESS CONTROL

Autor: Ortega Oria de Rueda, Iciar.
Director: Palacios Hielscher, Rafael.

RESUMEN DEL PROYECTO

Debido al continuo aumento de dispositivos del Internet de las cosas en uso, el hecho de que estos dispositivos estén conectados a la red y sean accesibles a través de internet desde cualquier parte del mundo supone una amenaza. Este proyecto busca definir un doble factor de autenticación basado en la posición del usuario para añadir una capa de seguridad que pueda aumentar la seguridad de los comandos IoT. En el caso de acciones no peligrosas, el sistema funcionara como normalmente, por medio de una validación estándar. Sin embargo, en el caso de cambios de configuración o comandos peligrosos, el sistema requerirá una autenticación.

La autenticación basada en la posición fortalece la seguridad causando únicamente una mínima molestia para el usuario, ya que los SMS, mensajes Push y códigos secretos son evitados.

Palabras clave: *IoT, Internet de las cosas, seguridad, localización, posicionamiento*

1. Introducción

Hoy en día, el Internet de las Cosas (IoT) se encuentra en continuo crecimiento. Esta tecnología está siendo usada en la mayoría de los aspectos de la vida del usuario y los dispositivos, anteriormente simples, están evolucionando, ya que están siendo dotados de inteligencia. Esto les aporta nuevas capacidades que los hacen más atractivos a los ojos de los usuarios, ya que hacen su vida más fácil. El numero de dispositivos IoT en uso en 2017 era entorno a 8.4 billones, contando tanto a consumidores como a negocios. Este número se espera que crezca hasta 20.4 billones para 2020 [1].

Este tipo de dispositivos se han abierto paso hasta las casas de los usuarios, sustituyendo a los dispositivos simples que los usuarios tenían previamente o añadiéndoles nuevas funcionalidades. Estos cuentan con gran cantidad de información sobre el usuario y sus costumbres, ya que son usados a diario por estos. Esta información les convierte en el blanco perfecto de ciberataques. Además, la seguridad en los dispositivos IoT no está siendo implementada a conciencia, dando lugar a numerosos ataques [2][3][4].

Uno de los mayores factores de riesgo de los dispositivos IOT es la comunicación con ellos a través de conexiones inalámbricas, que son intrínsecamente menos seguras que el acceso físico al dispositivo. Para reducir este riesgo, se debe aumentar la seguridad en los comandos enviados a través de estas conexiones.

2. Definición del proyecto

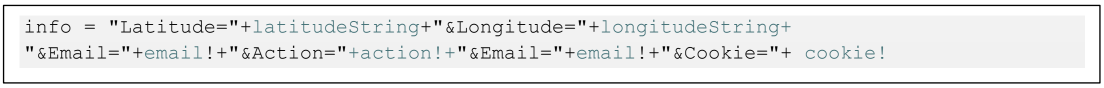
Como respuesta a esas necesidades, el objetivo de este proyecto es mejorar la seguridad de estos dispositivos del hogar cubriendo el agujero de seguridad que deja el acceso remoto. Para ello, el sistema propuesto emplea la localización del usuario para actuar como segundo factor de autenticación.

Limitar el acceso al dispositivo únicamente a la casa del usuario reduciría su utilidad, ya que una de las características más deseadas de estos dispositivos es la posibilidad del control remoto. Para crear esta nueva capa de seguridad empleando la posición, el sistema propone la creación de localizaciones seguras. Una localización segura es un área seleccionada por el usuario desde donde puede realizar determinados comandos de los dispositivos IoT que se consideran inseguros.

Debido a que el sistema emplea la posición obtenida a través del GPS del móvil, se ha realizado un estudio para probar la precisión y el retraso en el posicionamiento del usuario cuando se emplea el GPS.

3. Descripción del sistema

Para crear el sistema deseado, se ha hecho uso de una aplicación móvil creada para un sistema operativo iOS. Esta se conecta con un servidor a través de una conexión que emplea un protocolo HTTPS, tal y como se muestra a continuación:



```
info = "Latitude="+latitudeString+"&Longitude="+longitudeString+
"&Email="+email!+"&Action="+action!+"&Email="+email!+"&Cookie="+ cookie!
```

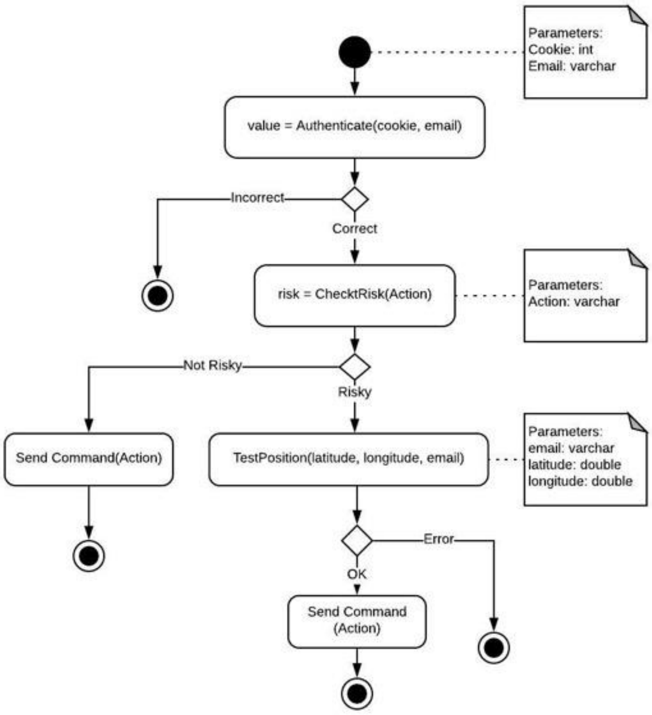


Ilustración 1 – Diagrama de Actividad del 2FA

El servidor estará encargado de comunicarse con el dispositivo IoT, situado en el hogar del usuario (este es el esquema que utilizan normalmente los fabricantes de dispositivos IoT). Para cumplir la funcionalidad, el sistema realiza las siguientes tareas, la mayoría de ellas realizadas en el servidor:

- Gestiona las tareas del usuario: crear y borrar usuarios, iniciar y finalizar sesión.
- Manejar las zonas seguras: agregar nueva zona segura, borrar una zona segura.
- Realizar el segundo factor de autenticación, si es necesario.
- Control de los dispositivos IoT: mostrar los que el usuario tiene registrados, añadir nuevos o borrar los que tiene.
- Dentro de los dispositivos, obtener la posición del usuario, y realizar peticiones de comando

4. Resultados

Se ha realizado un prototipo de una aplicación móvil de iOS y el código del servidor. En la Ilustración 2 se muestran las pantallas para crear una nueva localización y para manejar los dispositivos IoT con los que cuenta el usuario. Gracias a la aplicación, a través del servidor, el sistema es capaz de capturar la posición del usuario y comprobar si se encuentra dentro de un radio de 60 metros entorno a alguna de las posiciones que el usuario tiene almacenadas como "seguras".

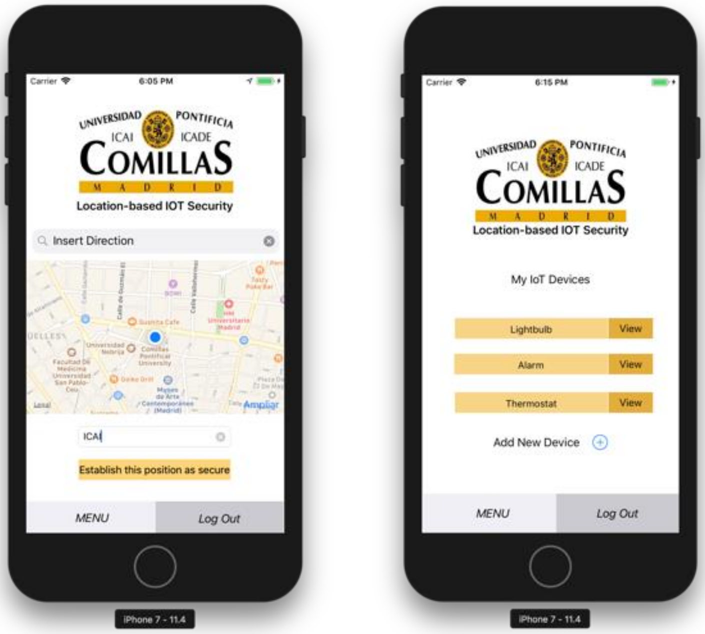

Carrier
6:05 PM
UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID
Location-based IOT Security
Insert Direction
Ampliar
ICAI
Establish this position as secure
MENU
Log Out
iPhone 7 - 11.4
Carrier
6:15 PM
UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID
Location-based IOT Security
My IoT Devices
Lightbulb
View
Alarm
View
Thermostat
View
Add New Device
MENU
Log Out
iPhone 7 - 11.4

Ilustración 2 – Ejemplos Páginas de la Aplicación móvil

La comprobación de la localización se realiza únicamente paras las acciones que están almacenadas en el sistema como arriesgadas, ya que las acciones no arriesgadas no requieren de este segundo factor de autenticación, con el fin de no limitar la funcionalidad de los dispositivos IoT.

Se ha realizado un estudio en las compañías de dispositivos IoT más populares y sus acciones fueron clasificadas como arriesgadas y no arriesgadas.

El sistema ha sido probado mandando comandos arriesgados y no arriesgados desde zonas "seguras" y zonas "inseguras".

5. Conclusiones

La seguridad de los dispositivos IoT no está siendo implementada como se debería. Muchos dispositivos IoT sufren continuos ataques para los cuales no están adecuadamente preparados. Estos dispositivos estás expuestos a estos ataques desde que están conectados a la red y se pueden acceder remotamente.

El sistema propuesto es capaz de proveer el nivel seguridad que da el acceso físico al dispositivo sin tener que limitar el acceso al dispositivo desde una única posición y sin eliminar acciones arriesgadas.

Este sistema está diseñado para funcionar como intermediario entre el dispositivo IoT y el verdadero transmisor de comandos. Los comandos no arriesgados pasan por el servidor y son enviados al dispositivo IoT como normalmente. Sin embargo, solo los comandos arriesgados que superen la segunda capa de autenticación serán mandados. Esto implica que no es necesario realizar modificaciones en el dispositivo IoT, ya que debe ejecutar todos los comandos que recibe del servidor.

El sistema diseñado es idóneo para las necesidades de estos dispositivos ya que proporciona una capa extra de seguridad sin apenas necesidad de intervención por parte del usuario (por ejemplo, no es necesario introducir una verificación), lo que lo hace más atractivo de cara a los usuarios, quienes normalmente ven el doble factor de autenticación como una molestia.

6. Referencias

[1] L. Tung, “IoT devices will outnumber the world’s population this year for the first time | ZDNet,” *ZDNet*, 2017. [Online]. Available: https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/.

[2] Steve Ranger, “ZDNet - What is the IoT? Everything you need to know about the Internet of Things right now,” *ZDNet*, 2018. [Online]. Available: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.

[3] J. Dyble, “97% of risk pros believe unsecured IoT could facilitate cyber attacks | AI | GigaBit,” *Gigabit Magazine*, 2018. [Online]. Available: https://www.gigabitmagazine.com/ai/97-risk-pros-believe-unsecured-iot-could-facilitate-cyber-attacks.

[4] T. Armerding, “Smart devices get smarter, but still lack security,” *CSO*, 2013. [Online]. Available: https://www.csoonline.com/article/2134252/fraud-prevention/smart-devices-get-smarter--but-still-lack-security.html.

IMPROVING THE SECURITY OF IOT DEVICES BY IMPLEMENTING A LOCATION-BASED ACCESS CONTROL

Author: Ortega Oria de Rueda, Iciar
Supervisor: Palacios Hielscher, Rafael.

ABSTRACT

Due to the constant increase on the number of Internet of Things devices being used, the fact that these devices are connected to the network and accessible through Internet from anywhere in the world imposes security threats. This project aims to define a two-factor authentication based on the user's location to create a new layer of security that increases the security of the IOT devices commands. In the case of non-risky operations, the system will work as usual with standard validation; however, in the case of configuration changes or risky commands, the system will require more advanced authentication.

Location-based authentication strengths security with minimal inconvenience for the user, since Text messages, Push messages and secret codes are avoided.

Keywords: *IoT, Internet of Things, Security, location, positioning*

1. Introduction

Nowadays, the Internet of Things is constantly growing. This technology is being used in most aspects of life and simple devices are evolving and getting endowed with Internet. The internet provides these devices with intelligence and gives them new capacities that make them more attractive to the user, as they make his life easier. The number of IoT devices in use in 2017 was around 8.4 billion, counting both consumers and business. This number is expected to grow up to 20.4 billion by 2020 [1].

This type of devices made their way into the user's home, substituting the common devices users previously had or adding new functionality. They hold information about the users and their habits, as they are used in their day to day. This information turns them into the perfect target for cyberattacks. Moreover, security in IoT devices is not currently thoroughly implemented, resulting in multiple attacks [2][3][4].

One of the highest risk factors of the IoT devices is the communication via wireless connection, that is intrinsically less secure than the physical access to the device. To reduce the risk, the security of the commands sent through these connections should be upgraded.

2. Project Definition

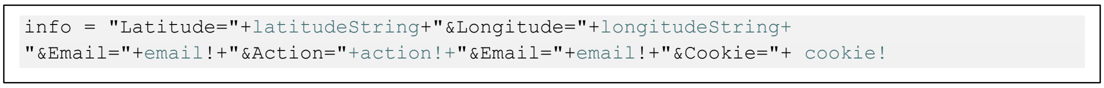
As an answer to these needs, the aim of this project is to upgrade the security of these home devices by covering the security hole left by the remote access. To do so, the proposed system uses the location of the user to act as a second factor of authentication.

Limiting the access to the devices to only the user's home would reduce the IoT devices usefulness, as one of their most liked features is the possibility of remote control. To create this security layer using position, this system proposes establishing secure locations. A secure location is an area, selected by the user, from where some commands of the IoT devices, those considered riskier, could only be performed.

As this system uses the location of the user obtained through the GPS of the mobile, a study of the accuracy of the user's positioning and the delay that it presents when the GPS is used, has been done.

3. System Description

To develop the desired system, a mobile application has been created for an iOS operative system that connects to a server through a connection using HTTPS protocol, as shown in Figure 1:



```
info = "Latitude="+latitudeString+"&Longitude="+longitudeString+
"&Email="+email!+"&Action="+action!+"&Email="+email!+"&Cookie="+ cookie!
```

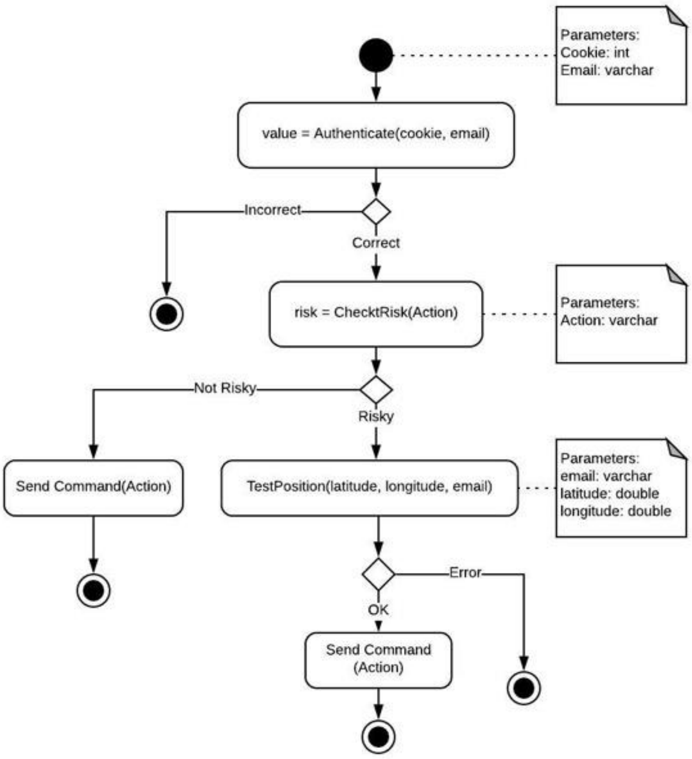


Figure 1 – Previous GPS Accuracy Study

The server will be in charge of communicating with the IoT device located at the home of the user (this is the scheme commonly used by IoT manufacturers). To accomplish the goals of the project, the system carries out the following tasks, most of them performed in the server:

- Manage the user tasks: add and delete users, log in and log out
- Manage the secure locations: add new locations, delete previous ones
- Perform the second factor of authentication on them, if necessary.

- Control of IoT devices: display the devices the user has, add new ones or delete.
- Inside of the devices, obtain user's position and carry out requests of commands.

4. Results

A prototype iOS mobile application and server-side code have been developed for demonstration and testing purposes. In figure 3, the screens to create a new secure location and the screen to manage the IoT devices are displayed. In this app, through the server, the system is able to establish the position of the user and check if it is located in a radius of 60 meters around any of the locations that the user has stored as 'secure'.

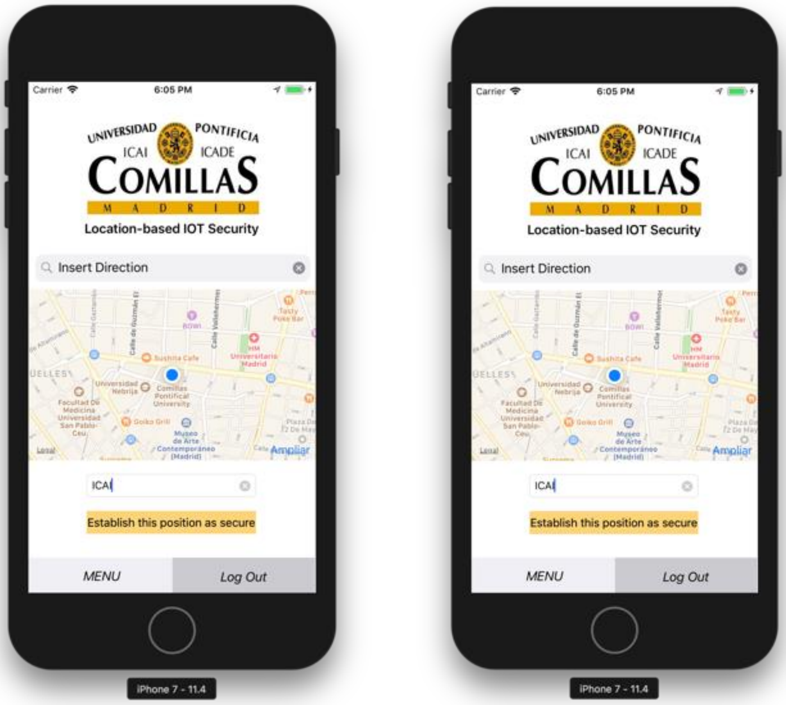

Carrier
6:05 PM
Location-based IOT Security
Insert Direction
ICAI
Establish this position as secure
MENU
Log Out
iPhone 7 - 11.4
Carrier
6:05 PM
Location-based IOT Security
Insert Direction
ICAI
Establish this position as secure
MENU
Log Out
iPhone 7 - 11.4

Figure 3 – App Examples

Location checking is only done for those actions that are stored in the system as risky, as not risky actions do not need this second authentication factor. This is done for the purpose of not limiting the functionality of the IoT devices with very standard actions.

A study was performed on the most popular IoT devices and their actions were manually classified as risky and non-risky. The system was tested sending risky and non-risky commands from 'secure' locations and from other locations and from other locations.

5. Conclusions

IoT devices security is not being implemented as conscientiously as it should be. Many IoT devices suffer constant attacks for which they are not prepared. These devices are exposed to these attacks since they are connected to the network and can be access remotely.

The proposed system is able to provide the security level of physical access without limiting the access to the device only to one place, and without eliminating risky actions.

This system is designed to serve as an intermediary between the IoT device and the actual command sender. Standard commands go through the server and are sent to the IoT device as usual. However, only those risky commands that pass the second layer of authentication are sent to the actual command sender. This means that no modification is needed in the IoT device, as it has to execute all the commands it receives from the server.

The designed system is ideal for the current needs as it provides an extra-layer of security without the need of almost any interaction on the user-side (e.g. no need to enter a verification code), which makes it more attractive to the users, who usually see two-factor authentication as an annoyance.

6. References

[1] L. Tung, “IoT devices will outnumber the world’s population this year for the first time | ZDNet,” *ZDNet*, 2017. [Online]. Available: https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/.

[2] Steve Ranger, “ZDNet - What is the IoT? Everything you need to know about the Internet of Things right now,” *ZDNet*, 2018. [Online]. Available: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

[3] J. Dyble, “97% of risk pros believe unsecured IoT could facilitate cyber attacks | AI | GigaBit,” *Gigabit Magazine*, 2018. [Online]. Available: https://www.gigabitmagazine.com/ai/97-risk-pros-believe-unsecured-iot-could-facilitate-cyber-attacks.

[4] T. Armerding, “Smart devices get smarter, but still lack security,” *CSO*, 2013. [Online]. Available: https://www.csoonline.com/article/2134252/fraud-prevention/smart-devices-get-smarter--but-still-lack-security.html.

Index of the Report

Index of Figures

Index of Tables

Chapter 1. INTRODUCTION

Nowadays, we live in a world where simple, common gadgets are rapidly making way for those endowed with intelligence. These gadgets are part of what it is called Internet of Things. The Internet of Things (IoT) devices are all kind of different devices that are now connected to the internet. This connection improves the utility of the devices, changing the way the user interacts with them and providing intelligence to these devices. IoT has come to make our lives easier [2].

Nowadays, the number of IoT devices is constantly increasing. In 2017, taking into account both consumers and businesses, there were around 8.4 billion IoT devices in use, a number which is expected to increase up to 20.4 billion in 2020. Approximately 63% of the total of IoT devices currently in use are consumer devices [1].

Users currently have IoT devices for a lot of different purposes but, one type that it is especially growing is the IoT devices for the homes of the users. This is aimed to achieve the concept of smart homes. Users have all sorts of IoT devices in their homes, from smart lightbulbs to smart thermostats, including smart locks. This proves that IoT is now a part of our lives and that its security is a precious matter, as our house safety depends on it.

For a great amount of IoT devices, one of the goals of the companies is to make these devices smaller and less expensive. This leads to a lack of user interface. The outcome of this trend is having all the devices connected to and controlled by the user's phone, by means of a local App. Also, the sensors use in IoT need to make use of cloud-based applications to be able to provide and utilize the information that they are receiving [5].

The result of using mobile applications is more flexibility, as an application can be coded to have a wider functionality. Unfortunately, it decreases the security of these devices, as the use of an application does not require physical access to it and it involves a wireless communication, which is intrinsically less secure. The lack of physical access may lead to some serious dangers in some actions performed in the device, so the goal of this system is to classify them and establish a two-factor authentication only for those that might be consider of higher risk.

The two factor-authentication adds an additional layer of security to the access of an account, resource or device. The majority of the most common used applications are now including the possibility to enable a two-factor authentication (2FA) mechanism to upgrade their security [6]. 2FA is seen as good practice in terms of security. With it, it is possible to combine different types of authentication (what you have, what you are, what you know). Despite this, many users do not like it as it can be disruptive to the user experience.

Currently, user's position is mostly obtained by GPS. The utility of this method is enormous and widely spread. GPS works with a connection to different satellites. The user gets connected to four satellites and they are used to calculate the distance to each of them and pinpoint the user's location. The downside for this project is that, as connection to the satellite gets more difficult in a closed area, it loses precision in a user's home [7].

1.1 MOTIVATION OF THE PROJECT

As mentioned before, the Internet of Things devices are making their way into users' homes. Their applications are countless and growing, both for consumers and businesses. One of these applications is predefining different scenarios or modes of operation to improve user experience. For this, the devices may detect patterns of action. This, combined with other applications, results in the IoT devices collecting sensitive data, as it may be used to reveal user behavior of the users. Moreover, the possibility of remote access to the device and the possibility of being connected to the network are threats that need to be considered.

Nowadays, security in IoT devices is not being taken as seriously as it should be [4]. This, combined with the sensible information the devices manage and the security risks that they may cause (e.g. a robbery due to a hacked smart lock), turns them into the perfect targets or instruments for cyberattacks [2][3][8].

Most of the Internet of Things devices that are in place now use Bluetooth and/or Wi-Fi to communicate, which is intrinsically less secure than direct hardware access. The wireless communication enables the remote control of the IoT device from the phone through an application. This possibility carries a danger, as an attacker can potentially perform actions in the devices, that may cause problems in the house. Some actions performed remotely by an attacker may be harmless, but others can cause a big problem to the user's home. As the devices are connected to the Internet, it becomes exposed to any attacker in the world.

A good example for an action that can be dangerous, and it is not needed to do remotely may be part of the temperature control. If the user lives in a really cold city, the heat cannot be turned off, as the pipes may burst. By deleting the possibility to vary the temperature, a smart thermostat loses most of its utility but, by regularizing what can and cannot be done remotely, the situation changes. It could be considered as risky just the action of turning off the heat or sending a great amount of orders to make a small change down on the temperature. To add a second layer of security to these risky actions, the user can prove that it is a valid user by sending the command from a trusted area. This increases the security as, in case an attacker has obtained the user's credentials, your device cannot be access from the attacker's position, but only from the user's trusted positions.

The purpose of this project is to reduce the possibility of attacks to home devices of the Internet of Things, without limiting its functionality and without hindering its use. Its main goal is to try to substitute the security provided by the physical access but with the possibility to control it remotely.

Chapter 2. DESCRIPTION OF TECHNOLOGIES

In this subpart, the technologies that have been used to deploy this project are going to be explained. First, the software part it is going to be explaines, along with the justification for its selection. Then, the same is going to be done with the hardware components.

2.1 SOFTWARE

This project is based mostly on the software part and does not count with a big amount of hardware. For the development and testing of this project, a mobile application has been designed and coded. The operative system that has been chosen for this application has been an iOS system. iOS system is Apple's operative system for mobile devices, such as the iPhone or the iPad. Although iOS is the second most popular system, after Android, it is considered highly secure. The reason of choosing iOS is the security it provides and the possibilities it offered, in order to test different variables of this project, as is the reminders by position. Due to the use of iOS, the language chosen to code the mobile application has been Swift. This has led to the possibility of profiting from the multiple libraries included. The environment chosen to create this has been the Xcode. The Xcode is an integrated development environment for macOS, operative system for Apple's computers.

In the server side of the application, Apache server and PHP have been used. Apache server is an open-source HTTP server. This is considered a secure, efficient and extensible server. As for PHP, it is a server-side scripting language. The choice of this language is due to the flexibility and capabilities it offers. In terms of the database, MySQL has been used as a database manager, as it is open source and it works smoothly with PHP.

2.1.1 XCODE AND SWIFT

XCode is a built-in development environment for MacOS that has all the tools developed by Apple to be able to create software for Apple apps. It has been chosen because it come with multiple frameworks that ease the design of the iPhone Apps.

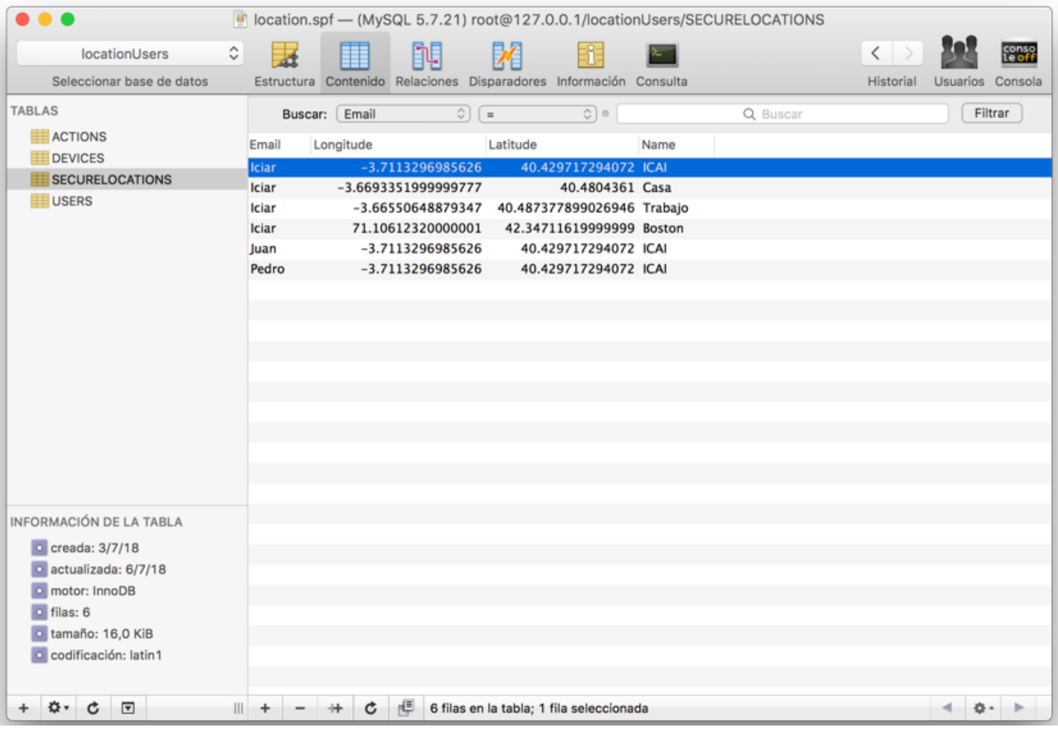
On his side, Swift is a powerful programing language for MacOS, iOS, watchOS and tvOS. Currently, it is using Swift 4, the newest version of Swift.

2.1.2 PHP

PHP is considered to be one of the most powerful programming languages. It is widely used so, either officially or created by the users, there is a lot of documentation about it. PHP is multiplatform which makes it very flexible and enables the server to be in any operative system. PHP counts with very useful functions to encrypt and decrypt information, as well as hashing functions, which was needed in order to safely store user information (passwords). All server-side coding has been written in PHP.

2.1.3 SEQUELPRO. SQL AND MYSQL

For this app, there was a need to create a database. As the information is simple and does not need to be really scalable, the final choice was to choose SQL, the most used language for Relational Databases. Taking advantage of the syntaxes, the methods what has being used is commands like CREATE TABLE, DROP TABLE, SELECT, INSERT, UPDATE, DELETE and the relations between the databases have mostly been done thanks to SQL statements. To interact with this database, what has been used is Sequel Pro. Sequel Pro is a fast, easy to use and native Mac OS application to manage databases. It gives direct access to MySQL Databases on remote and local servers.



location.spf — (MySQL 5.7.21) root@127.0.0.1/locationUsers/SECURELOCATIONS

Buscar: Email =

Email	Longitude	Latitude	Name
Iciar	-3.7113296985626	40.429717294072	ICAI
Iciar	-3.6693351999999777	40.4804361	Casa
Iciar	-3.66550648879347	40.487377899026946	Trabajo
Iciar	71.10612320000001	42.34711619999999	Boston
Juan	-3.7113296985626	40.429717294072	ICAI
Pedro	-3.7113296985626	40.429717294072	ICAI

INFORMACIÓN DE LA TABLA

- creada: 3/7/18
- actualizada: 6/7/18
- motor: InnoDB
- filas: 6
- tamaño: 16,0 KiB
- codificación: latin1

6 filas en la tabla; 1 fila seleccionada

Figure 1. Sequel Pro

2.2 HARDWARE

The hardware part of the project counts uniquely with the IoT device that the user may have, and with a Beacon, as part of the study on how to improve the precision of the system. A USRP has been also used for another study.

2.2.1 BEACON

A beacon is a small device that broadcasts a short-range signal based in Bluetooth, specifically in this case Bluetooth Low Energy. Bluetooth Low Energy (BLE) is a wireless personal area network technology. The main difference with the commonly used Bluetooth is that it reduces power consumption and cost. BLE is turning out to be very useful for multiple application and it is being widely used in mobile applications. BLE has 40 physical channels in the 2.4GHz ISM band, each separated by 2GHZ. It can both transmit data or just advertise [9]. Beacons can transmit location, as well as weather or other data. In this case, the beacon is used to advertise its location.

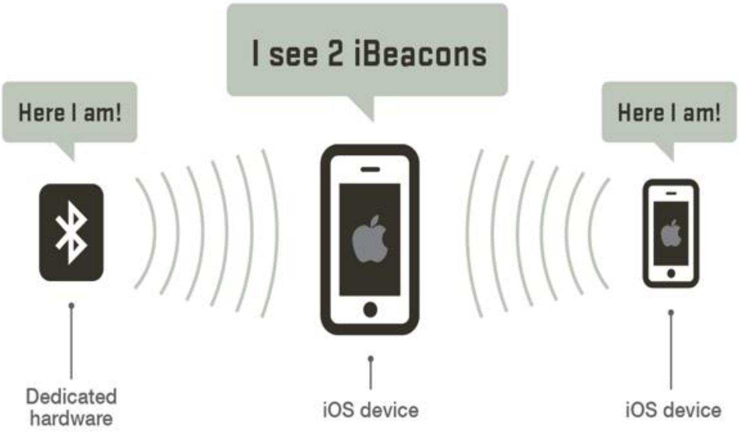


Figure 2. iBeacon Behaviour

The specific device that is being used is Radius Networks RadBeacon Dot. It comes with and adjustable range of 5-50m and an adjustable advertisement rate of 1-10Hz. The version of the Bluetooth connection is the 4.0 (Bluetooth Smart). It works with both Android and Apple and comes with an integrated PCB as the antenna. In this case, as iOS is being used, the protocol in use is iBeacon. iBeacon is Apple's technology standard to allow the iOS mobile applications to understand the position sent by the Beacon [10].

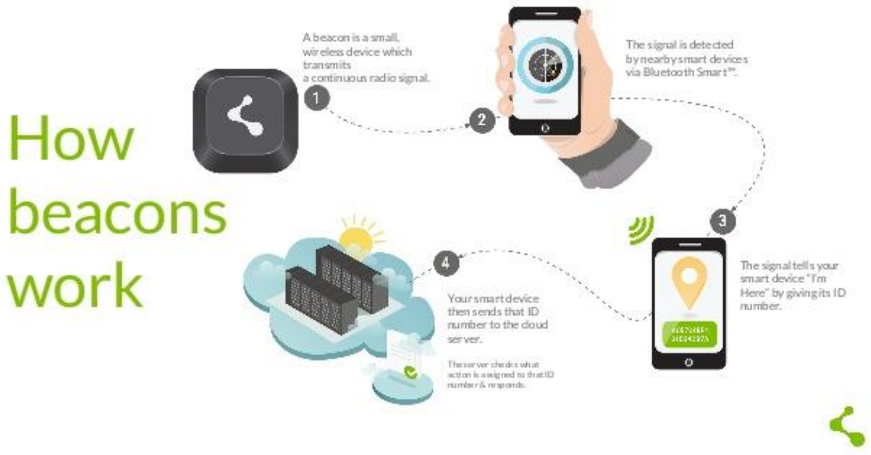

How beacons work
1
A beacon is a small, wireless device which transmits a continuous radio signal.
2
The signal is detected by nearby smart devices via Bluetooth Smart™.
3
The signal tells your smart device "I'm Here" by giving its ID number.
4
Your smart device then sends that ID number to the cloud server.
The server checks what action is assigned to that ID number & responds.

Figure 3. How Beacons Work

2.2.2 USRP B200

For one of the methods studied to improve the system, a USRP B200 has been used. USRP is a Software defined radio (SDR). It provides a fully integrated, single board, Universal Software Radio Peripheral platform with continuous frequency coverage from 70 MHz –6 GHz. It will intercept and decode the LTE packets between the cell tower and the mobile devices.

Chapter 3. STATUS OF THE MATTER

This project is designed to act as an intermediate between the user sending the commands to the smart device and the system that actually sends them to the device. These devices have a variety of communication standards in use, some of them not commonly known. As a way of interacting with them and translating the protocols, a solution has been proposed: Home Hubs. A home hub is a particular hardware device that is connected to all the different IoT devices at home and manages the communication using different technologies (WiFi, Bluetooth, Thread, Zigbee, Z-Wave, KNX, and more) and protocols. One of the greatest advantages of this device is the functionality know as: IFTTT (If This Then That). This gives the user the possibility of creating chains of events, i.e. triggering actions when a particular situation, change or action occurs. Despite all the perks of a Home Hub, it is not really popular amongst users, as, to the public eye, they are too expensive for a device that does nothing by itself.

The home hubs are being replaced by smart speakers equipped with integrated virtual assistants. They let the user control several smart devices with their voices to, for example, set an alarm or play music. Some of these devices do need a phone to have the assistant listen and some do not. This does require the user to be present and the capabilities are more reduced that what intended in our project. With this, the devices can only be activated locally. Our goal is to stablish multiple safe areas from where the user can access the devices. With this, the performance of the risky commands is not limited uniquely to a user's home, as it would turn it into a common device, but to as many areas as the user wants.

Most of the Internet of Things devices that are now in place use Wi-Fi to communicate. This facilitates the communication with the mobile phone and it is the key element that opens the possibility of controlling the IoT devices from the user's phone. This remote control is what exposes the user's home to external threats as, with it, it is connected to the internet. Any attacker, from anywhere in the world, could access our home gadgets if he is in possession of the right credentials. Theft of credentials has occurred too many times by now.

In terms of utilizing the user's position in IoT, there have been some studies. However, this has mostly been explored to enhance user experience or to endow the devices with new capacities. One of the most known applications of location for IoT is to control the position of the assets to reduce theft or loss [11]. Another common used of the position is for the mobile application that utilize the location-based services (LBS). This can be used for multiple purpose, from vehicle tracking to health applications.

The idea illustrated by Rezazadeh et al. also explores the use of positioning the user combined with Internet of Things devices. It suggests that using both the position of the user inside a shopping mall and the data obtained from different IoT smart object, can be profitable, comfortable and beneficial for both the costumers and the establishments. This is an example that, as it has been mentioned before, the combination of IoT and position is being explored, but not in terms of security.

The named systems have all been tasted in inside environments. They work with technologies such as Wi-Fi, Bluetooth Low Energy or sensors in the client-side. This is due to the fact that GPS is not reliable to precisely locate users in a closed area. While the accuracy of the GPS for client-based indoor position is between 5 and 20 meters, accuracy for Wi-Fi is 5-15 meters, for BLE (beacons) is 1-3 meters and for Li-FI (VLC) is under 50 centimeters [7].

Chapter 4. DEFINITION OF THE PROJECT

4.1 JUSTIFICATION

The smart homes are gaining popularity and expanding horizons. New, innovative devices, are constantly coming up. All sorts of before simple devices are getting endowed with intelligence. These devices are connected via wireless signals to the user's mobile device, for the purpose of being managed and to provide flexibility on their usage. This wireless connection makes the remote control possible, which is translated into a lack of physical access from the user side. In the past, to disarm an alarm, the user needed to be inside of the home. With the wireless connection of a smart alarm, the user can disconnect it from anywhere, the same as an attacker could if he gains access to the credentials.

An attack on a smart home device should be a big concern when talking about IoT. An attack that access a home device could result in a dangerous breach of security for a user's home. It is not needed to explain the importance a user puts on the security of his home. The objective of this project is to enhance the security of the IoT devices for a better protection of the user's home. This is going to be developed focusing on correcting the risks of the remote control, without eliminating that feature, but reducing the functionality.

The two-factor authentication (2FA) is an improvement on security, but most users are not actually happy about its implementation. Users see the second factor of authentication as a disadvantage, as it is an "obstacle" on their user experience. This is why this project has aimed to make that upgrade on the IoT devices security in a non-disruptive way, so that users take advantage of the new security layer, but without the need to constantly 2FA authenticate in each command sent to the IoT device.

4.2 GOALS

What it is mainly aimed at this project is to achieve a simple, secure, non-disruptive two-factor authentication for critical actions on IoT devices using the position of the user at the moment of the command, instead of an SMS. The main goals are:

i. Analysis of different devices, stablishing which actions can always be accepted (not risky), and which ones need further verification (risky).
ii. Study of current two-factor authentication techniques
iii. Development of a mobile application to determine the position of the user and analyze the precision of this location.
iv. Present the concept of secure location and establish them. Implement the web-server application to manage actions.
v. Analysis of different methods to improve reliability.

4.2.1 ANALYSIS OF DIFFERENT IOT DEVICES AND CLASSIFICATION OF ACTIONS

Currently, the range of IoT devices available in the market is humongous. In this project, the focus is placed on smart devices for homes. These devices count with a lot of different features and not all of them present a thread to the user's security. The goal of this study is to differentiate which of those are consider risky and present the need of further authentication. The restriction on the location of performance of these actions also shouldn't limit the functionality of the device.

4.2.2 STUDY OF CURRENT TWO-FACTOR AUTHENTICATION

Currently, two-factor authentication is widely implemented in lot of different sectors, i.e. financial, industrial. In the use of two-factor authentication, there is a wide range of options in methods to choose to implement in each factor, as there are multiple types of authentication factors. This study is aimed to get to know what combinations of factors are currently being used which ones the users prefer and why to see how the project would work on the market.

4.2.3 MOBILE APP

The mobile app is the main part in terms of usage of the project. The app is a demonstration of how the project should look like and work. It is the practical part of the project and shows how both the user and the system would interact with the IoT devices and how the security method would influence on the user experience.

4.2.4 SECURE LOCATIONS

One of the main focuses of these project is to set the concept of secure locations. All the security of the project is based in establishing secure locations. This is why this concept needs to be clearly explained. A server is going to be deployed to show how they would work.

4.2.5 DIFFERENT METHODS

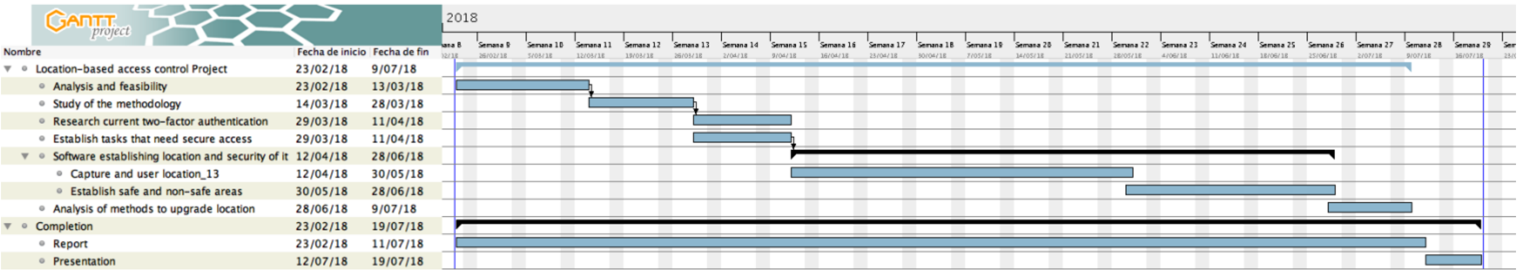
In this project, there is going to be a study of how this security method could be improved to make it more trustworthy and precise. The idea is to search for other non-disruptive methods that could be used to improve the security of the IoT devices.

4.3 WORK METHODOLOGY

This project has been developed according to an agile methodology. An agile methodology adapts to changes, it provides flexibility, gives the opportunity of an early delivery of the project with continuous changes to improve the product. With this, both the studies and the application have been developed and obtained progressively, with continuous goals, to have always a working system, in which capabilities have been added up. This has been chosen this way to allow us to see how the project progressed. [12]

4.4 PLANNING AND ESTIMATED EXPENSE

Due to the fact that an agile methodology has been used, the planning of the project has been structured is short tasks that leave a closed product after each one. The most striking feature of the planning is the division of the tasks based on the main objectives of the project, i.e. research of two-factor authentication, establish tasks that need secure access, etcetera. The planning is shown in Figure 4.

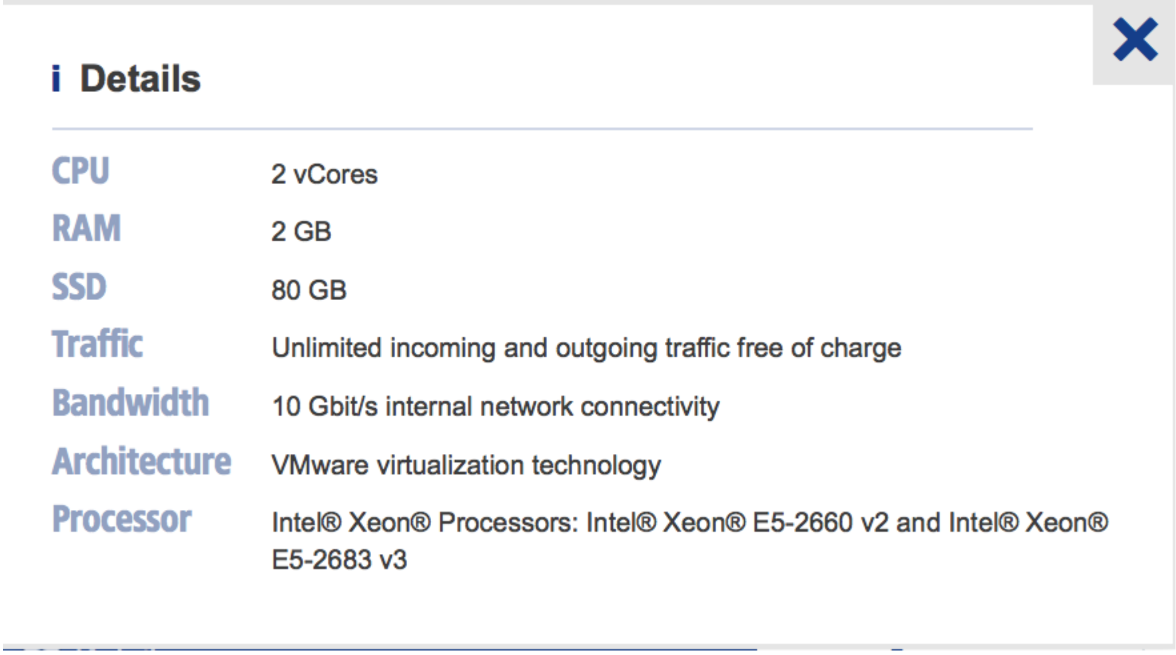


Nombre	Fecha de inicio	Fecha de fin
Location-based access control Project	23/02/18	9/07/18
Analysis and feasibility	23/02/18	13/03/18
Study of the methodology	14/03/18	28/03/18
Research current two-factor authentication	29/03/18	11/04/18
Establish tasks that need secure access	29/03/18	11/04/18
Software establishing location and security of it	12/04/18	28/06/18
Capture and user location_13	12/04/18	30/05/18
Establish safe and non-safe areas	30/05/18	28/06/18
Analysis of methods to upgrade location	28/06/18	9/07/18
Completion	23/02/18	19/07/18
Report	23/02/18	11/07/18
Presentation	12/07/18	19/07/18

Figure 4. Gantt Diagram

In terms of expenses, the estimated cost to design the following design is divided in cost of work and cost of infrastructure:

- In terms of the employment, a programmer has been needed to implement the project, both for the app and the server. This leads to the need of paying a salary, which is 2480 € per month, as a mean for a software engineer in Spain.
- Server: for the testing, it has been developed in localhost but, for a real use, a cloud-server should be used. A good server that could be used is 1and1 server. Assuming a great number of users, an L server should be used. The price of this server is 19,99€/month and it has the characteristics shown in the following figure (Figure 5). Using two servers would result in 39,98€ each month.



i Details

CPU	2 vCores
RAM	2 GB
SSD	80 GB
Traffic	Unlimited incoming and outgoing traffic free of charge
Bandwidth	10 Gbit/s internal network connectivity
Architecture	VMware virtualization technology
Processor	Intel® Xeon® Processors: Intel® Xeon® E5-2660 v2 and Intel® Xeon® E5-2683 v3

Figure 5. Cloud Server Information

- Client-side: as a method of enhancement of the precision of the location of the user, the user could purchase a Beacon. The one purchased for testing, which was really simple, is value in 11,5€. The user also needs to acquire the IoT devices, but those are not part of the price of the system.

	Price to develop (MONTHLY)
Programmer	2480 €
Server	39,98 €
Total	**2519,98 €**

Table 1. Cost Estimation

Chapter 5. STUDIES

5.1 ANALYSIS OF TWO-FACTOR AUTHENTICATION METHODS

Two-factor authentication is a security method that consists on adding a second layer of authentication to improve the security of the system. It is similar to what, in terms of security, is called *Defense in Depth*. The concept of defense in depth is based on a layered security mechanism where the main goal is that, if the system is attacked and the attacker can surpass a security layer, he/she would stumble with another layer of security, making it harder to compromise the system. In this method, the idea is that the methods can complement each other [13].

In terms of security, the authentication factors can be of three different types: possession factor (what you have), biometrical factor (what you are) or knowledge factor (what you know). An example of each one is:

- Possession factor: a fob that randomly generates a code each 30 seconds
- Biometric factor: fingerprint (TouchID)
- Knowledge factor: the most commonly used, the user/password scheme.

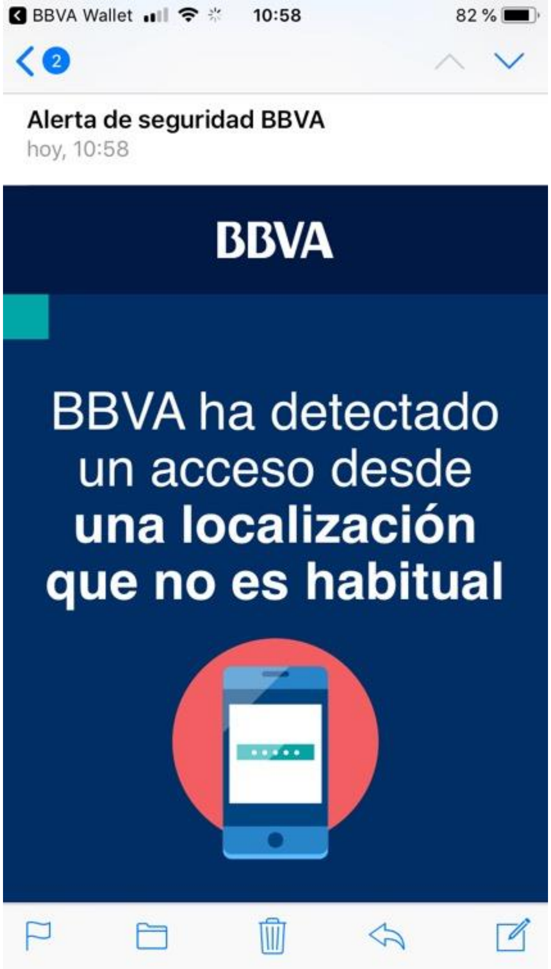
The two-factor authentication aims to strengthen the security of the system by combining two types of credentials to access the system. Currently, two-factor authentication is widely implemented. The combination of what you know (username and password) plus what you have (a mobile phone where you can receive an authentication message) is currently being used by banks, when the user wants to make a payment via internet, or by mobile applications, for verification of the user's identity, for example.

Each security method has its strong points and its flaws. Two-factor authentication should be implemented in a way that the methods cover each other's flaws. Below, different, currently used, authentication methods are shown, along with some of their flaws and strong points [14].

- Push Notifications: mobile app, specially designed for this use, where the user can approve an authentication by accepting the access attempt displayed on a push notification on the mobile phone. This requires the user to carry a mobile phone.
- Security Tokens: A security token is a small hardware device that, once the user inserts a PIN, it displays a pseudo random number. This number changes in time and, if inserted on the system, it grants access to the user to it. Security tokens have the advantage that, even if the user forgets the phone or is out of service, the system can still be accessed. An example of a security token can be a key fob [15]. The problem is that, in case the token is stolen, the thief could give access for himself to any of the different systems that the user has on the phone.
- SMS Passcodes: After the first authentication layer, the user receives a passcode in a SMS and has to enter it to finish the process. This is useful in case the user does not have Internet connectivity but has mobile signal. Also, SMS are difficult to intercept.
- Phone Callbacks: Another method used, less common, is to identify the user through a call to a phone provided by the user. To authenticate, the user has to answer the phone and press a key previously selected by him to approve it.
- HOTP and TOTP: HMAC-based one-time password and time-based one-time passcode are two types of passcodes obtained through an application that the user needs to introduce in the application that he is trying to access. The TOTP is valid through a small amount of time (typically between 30 and 60 seconds).
- Universal 2nd factor Device: This factor is commonly used in the industry. It is the standard for two-factor authentication. It can be integrated in different devices (devices using USB, NFC, Bluetooth) and in different forms. One of the most popular is through an USB device. The user has to plug it in and then, he can access the account he has the U2F for. It uses key cryptography.

This list is just a brief summary of all the two-factor authentication methods that are currently been used. The list of different methods is too wide to be totally covered. There are hundreds of them [16].

The proposed system is focused on domestic IoT devices. It tries to increase security by limiting remote actions on those home devices. However, this idea could be extrapolated and implemented on other sectors (financial, industrial…). The financial sector was a pioneer in the implementation of two-factor authentication or 2FA. Most personal banks today, allow their clients to check balance and search recent transactions just with basic credentials such as login and password. However, to get deeper into account information, send a wire transfer, change settings, etc. the system will require a second factor of authentication. This technology has also been applied to other system, mostly to protect users from stolen passwords. Almost all sectors have adopted two-factor authentication technology in some extent, being the IoT sector one of the exceptions [17]. Although almost all current 2FA systems rely on Text Messages (SMS) sent to mobile phones, the proposed method uses the phone's location as the second factor. One of the advantages of using location is that the system increases security in a very transparent way, without bothering the user with text messages, phone calls, and security codes. In fact, some location information (at lower resolution) has been used as a way of fraud detection in the financial sector, by detecting web access to banks from unexpected Internet locations (Figure 6) or use of credit cards in different cities/countries [18].



BBVA Wallet 10:58 82 %

Alerta de seguridad BBVA
hoy, 10:58

BBVA

BBVA ha detectado un acceso desde **una localización que no es habitual**

Figure 6. Unsual Activity Notification

5.2 Classification of tasks on different IoT devices as Risky/Not-Risky

A risky action is an action that may cause a great damage to a user's home or that, if compromised, may present a big threat on the user's home security. Also, for the proposed system, these actions need to have the characteristics such that, if the functionality is limited to certain areas, it does not affect enormously on the usefulness of the IoT device. Below, there is a small sample of home IoT devices from different companies where the features have been extracted and classified as risky or not risky.

5.2.1 NEST DEVICES

NEST is a home automatization producer, founded in 2010 in California. It was a pioneer company in IoT devices. It was cofounded by Tony Fadell and Matt Rogers, who are currently Apple engineers. It is now merged with Google's Hardware Unit [19]. The goal of the company, as they describe it, is to "create a home that takes care of the people inside it and the world around it" [20]. Following, there is a classification of the features of the different NEST devices.

Figure 7. Nest Thermostat

- Thermostat

- NOT RISKY:
  - It can use sensors and the user's phone location to check if the user has left, and then, change temperature according to a pre-defined value.
  - Learn the pattern of the user temperature changes.
  - With a sensor , the user can give rooms priority when regulating the temperature.
  - Adjust temperature remotely.

- RISKY

  - Control the heating and cooling system and give you alerts, i.e. if temperatures are too low in winter your pipes could burst. The management and limitation of this feature can be considered risky.
  - Big changes on temperature or continuous commands of small changes (it can turn off the heat and make the pipes burst)

- Cameras

Figure 8. Nest Camera

- NOT RISKY
  - Outdoor camera
    - Detect a person up to 50 feet away, then alert the user with a photo of who’s there
  - Indoor Camera
    - It includes a speaker for the user to scare off intruders from afar. It also counts with noise cancellation and echo suppression, so the user can hear them loud and clear.
    - Nest Cam IQ plugs into power, so it won’t run out of batteries before it sends an alert.
    - With Supersight, Nest Cam IQ can zoom in on someone walking across the room, while still showing the full picture to the user.

- RISKY
    - Indoor and outdoor camera
        - See key snapshots from the last three hours of activity in the Nest app, as it can invade the user's privacy if access by an attacker and it the user does not need to do this from anywhere.

- Doorbell

Figure 9. NEST

- NOT RISKY
    - 24/7 continuous recording
    - Person, motion and sound alert to detect visitors
    - Recognize family and friends and send special alert
    - Prerecorded quick responses
- RISKY
    - Personalization of actions for familiar faces

- Alarm system

- NOT RISKY
    - Get a Remind Me alert so the users can arm it right from the phone in case they have forgotten.
    - Get security alert to verify what's happening.

Figure 10. NEST Alarm System

- RISKY
  - Set a schedule to let someone in at certain times, as an attacker can configure a schedule and the alarm will disarm whenever they want without been seen as an abnormal action.
  - Users can choose how long it takes for the alarm to arm. This is risky as the attacker could set a really long time, giving time for an attack. Some alarms tell you how much time you have left, so in that case it should be less problematic, but users may not pay attention to the message.

- Lock

- NOT RISKY

Figure 11. NEST Lock

  - Let someone in (disarm the alarm). It is a risky action, but its limitation cuts off the functionality of the system.
  - Get alerts whenever someone unlocks and locks the door.
  - The door can lock automatically if the user is not home.

- RISKY
  - Create passcodes for family, guests and people the user trust. It is risky as it gives access to whoever the user wants, and the attacker could grant access to himself. The limitation of this function does not reduce the functionality of the system.
  - Set times for passcodes to expire. An attacker could set really low times, resulting in a denial of service (DoS attack) or set one too long so he has more time to hack the system.

- Smoke + CO alarm

Figure 12. NEST Smoke

- NOT RISKY
  - Gives the user a heads up if something is not right but it's not too dangerous.
  - Tells the user where the problem is.
  - Test alarms

- RISKY
  - Configure who receives a message when something is wrong

5.2.2 BELKIN DEVICES

Belkin inception was in 1983. It was founded by Chet Pipkin. He started selling cables for computers. It was not until 2012 when WeMo was founded. WeMo is Belkin's home automatization line. Following, there is a study of a Belkin device [21]. Belkin counts with more devices but most of them are similar to Nest's and the have the same, or less features, so they are not going to be analyzed, as the classification will give a similar result.

- Wemo® Insight Smart Plug

- NOT RISKY
  - Obtain real-time reports on how much energy our devices are consuming.
  - Provide wireless control of lamps, heaters, fans, etcetera, using home's Wi-Fi.
  - Control any device connected to the plug

Figure 13. Wemo Insight Smart Plug

- RISKY
  - Schedule the devices connected, as an attacker could create a schedule and turn on the plug without the user noticing, connecting devices that may be dangerous, creating discomfort or raising the user's energy consume.
  - Enable randomized lights when the user is not home to scare away thieves. As the user is not home, he/she may not notice this happening and it may create an almost constant light pattern, raising the consume. This is an action that is not urgent, it is not needed to do it from anywhere, so it can be limited without problem.

5.2.3 SENSIBO DEVICES

Sensibo was founded in 2013 by Omer Enbar and Ran Roth. Sensibo is an IoT company that produces smart air conditioners. They raised the money they needed for the company thanks to a crowdfunding campaign in 2014 [22].

- Air conditioner

- NOT RISKY
  - Control air conditioner from anywhere. Small changes should be allowed.
  - Monitor the temperature and humidity remotely
  - The air conditioner turns on automatically before the user arrives, turns off when the last person leaves using the user's phone geo-location

Figure 14. Sensibo Smart Air Conditioner

- RISKY
  - Big changes of temperature or continuous small changes should be monitored and limited.

5.2.4 PHILIPS DEVICES

Philips is one of the most important technology enterprises. It was founded in 1891 but it was not until recently that they started manufacturing IoT devices. In Philips there are multiple devices for home automatization [23]. Most of them has been previously explored, although they were from another brand. Following, there is an analysis of their most different devices.

Figure 15. Philips Hue

- HUE

- NOT RISKY

  - Control the lights remotely
  - Enable wake-up lights

- NOT RISKY

  - Light schedules. Any type of scheduling action is not considered secure as it normalizes the actions made so the user does not notice. Also, it is not an urgent action, it does not require that the user can do it at any time, so it can be regulated.
  - Create scenes. Same thing happens with the scenes, as an attacker could obtain the pattern of action of the user, as well as establish a new one that may include dangerous actions.

5.3 SECURE LOCATIONS

In this part, the concept of *secure locations* is going to be precisely explained, as well as how it is going to work, and how the server is going to manage it.

A secure location is a new concept introduced and used in this project. As the security method of this project is based on the location of the user and the idea of the project is to control it but not completely restrict it, there is a need to establish some ways to differentiate positions. There appears the concept of secure locations. A secure location is an area (the radius will be later discussed and explained) that the user choses, from where he can send any command, both risky and not risky, and the system will execute it. A secure location could be any position chosen by the user. With this, the lack of physical access is made up for, as the user needs to be in a concrete place, but it does not take away the remote-control possibility, as the user can define where he would need to access the device and can establish as many secure locations as needed to do it.

When the user is starting to configure the system, he can choose the first secure location from wherever he needs but, once he has created a secure location, all the following secure locations need to be selected from another secure location. With this, we want to prevent the possibility that an attacker may gain access to the system and establish a convenient place to perform an attack, bypassing the proposed security method.

5.3.1 GPS ACCURACY STUDY

To capture the security location, this system uses the GPS incorporated on the user's mobile phone. With this, the application captures an approximate point of where the user wants to establish the position. GPS is a reliable method commonly used to track the user's position. The problem with the use of GPS in the proposed system is that we are designing it for a home, so it is very likely that the secure locations selected by the users are closed places (at least the home where they are using the system). This results in the GPS location losing precision. GPS cannot be relied to give a really precise location when it comes to a closed environment. This is caused by how the GPS works, because satellite signals are too weak and do not travel well through structures.

GPS (Global Positioning System) is a system based in 24 satellites that can provide location information from anywhere in the planet. The GPS receiver (user's phone in this case) needs to be able to contact with at least four receivers. These four receivers are used to establish the user's position. The satellites send a signal containing their position and the time when the signal was send. As the GPS receiver "knows" where the satellites are and how long it took for the signal to arrive, it can pinpoint the user's position by triangulation. The precision of the GPS is said to be between 10 and 20 meters. This is notably decreased when the user is in a close area [24][25].

As a test to prove the precision of the GPS, a walk has been recorded thanks to the mobile app Geotag Photos. This track is made both through open and closed areas in two different scenarios: with Wi-Fi and without Wi-Fi. In the following images, these two scenarios, as well as an image of what the real path looks like, are shown. It has to be pointed out that, in these paths, the user is located in a university campus where the Wi-Fi is distributed in different buildings but is the same for all of them. In all the figures, the points recorded in

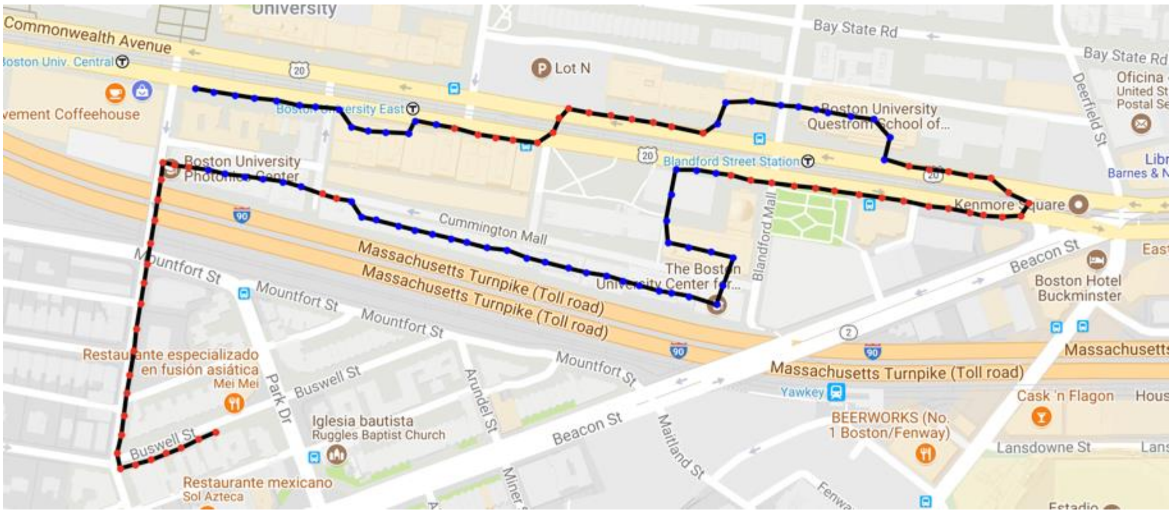


Figure 16. Real Path. Blue Dots = Inside. Red Dots=Outside

parts where the user walks in closed areas are marked in blue and parts where the user walks through open areas are marked in red. Figure 16 shows the real path walked by the user.

Now, we are going to show and analyze the case where the user is connected to the Wi-Fi (Figure 17). Wi-Fi is typically used to improve position accuracy, specially inside building or without good GPS reception. In this case, Wi-Fi is located in some of the buildings, what makes the GPS jump from one building to another, as the fact of being connected to one Wi-Fi is seen as the user being in the position where the router is located or near it. Also, whenever the user got into a closed area and the mobile phone could not connect to the wi-fi, it could not establish the position and did not it, reducing considerably the number of points.

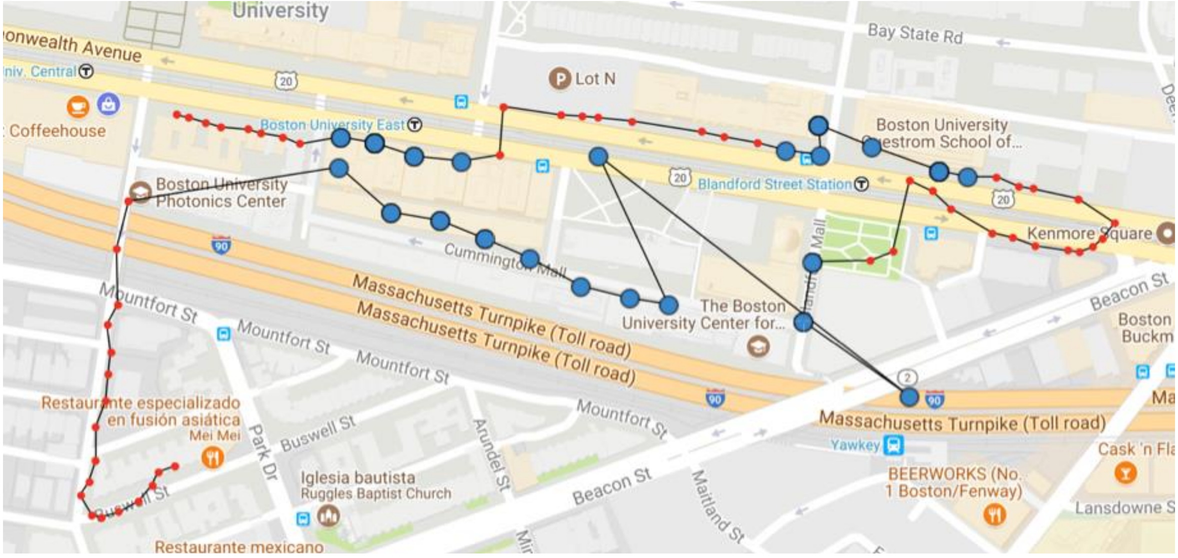

University
onwealth Avenue
niv. Central
Coffeehouse
Boston University East
Lot N
Bay State Rd
Boston University Questrom School of...
Blandford Street Station
Kenmore Square
Boston University Photonics Center
Cummington Mall
Massachusetts Turnpike (Toll road)
Massachusetts Turnpike (Toll road)
Mountfort St
Mountfort St
Mountfort St
Mountfort St
The Boston University Center for...
Beacon St
Beacon St
Boston Buckm
Restaurante especializado en fusión asiática Mei Mei
Park Dr
Buswell St
Buswell St
Iglesia bautista Ruggles Baptist Church
Arundel St
Maitland St
Massachusetts Turnpike (Toll road)
Yawkey
BEERWORKS (No. 1 Boston/Fenway)
Cask 'n Fla
Lansdowne S
Restaurante mexicano

Figure 17. Path with Wi-Fi

It has to be taken into account how this has been obtained. The real time when the user made a turn was recorded and from that, the turning points have been leveled and the straight parts of the path have been compared, so the points may not be compared with the exact same one in the other path, as there may be more points in one straight line than in the other. From this comparison, the mean distance error obtained has been of 73.5 meters. The minimum distance error obtained is 8.3 meters and the maximum are 200.1 meters. A graphic of how the distance error varies can be seen in Figure 19. The error varies in a wide range but most of it is located under 100 m.

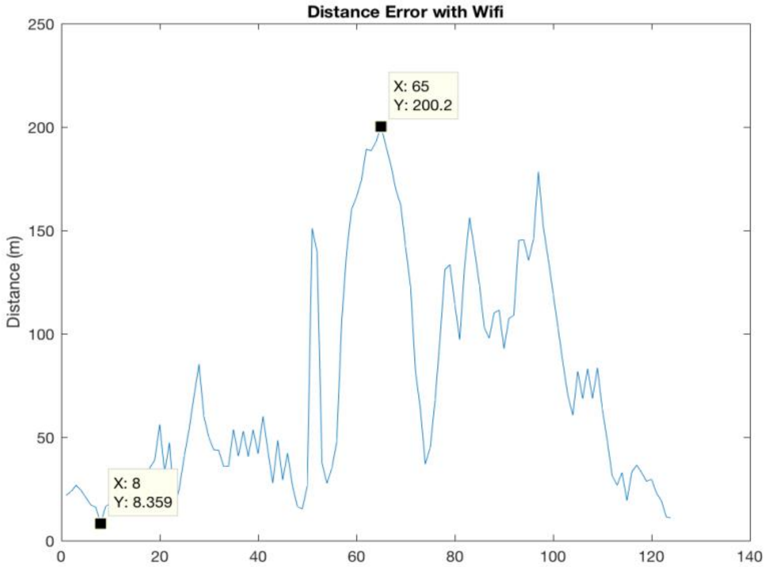


Figure 19. Distance error with Wi-Fi

The mean-squared error has been tested both in the latitude and longitude for this path. Mean-squared error (MSE) is an estimator of the performance of a prediction. Mean-squared error is defined as the average of squares of the "errors" [26]. The closer this value is to zero, the better is the prediction. In the case of the latitude, the mean-squared error is of approximately 5.6e-08, meanwhile, the mean-squared error of the longitude is of 1.1e-06, being this one higher. What this indicates is that the deviation in the error of the latitude is lower than the one for the longitude, but both of them pretty good.

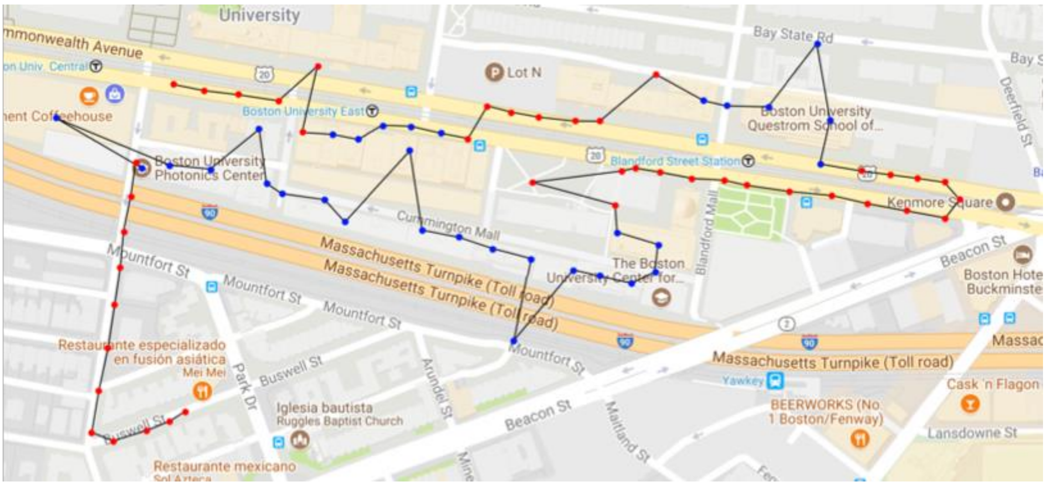

University
mmonwealth Avenue
Bay State Rd
Lot N
Boston University East
Boston University Questrom School of...
Boston University Photonics Center
Blandford Street Station
Kenmore Square
Cummington Mall
Massachusetts Turnpike (Toll road)
Massachusetts Turnpike (Toll road)
Mountfort St
Mountfort St
Mountfort St
Mountfort St
The Boston University Center for...
Blandford Mall
Beacon St
Beacon St
Boston Hotel Buckminster
Massachusetts Turnpike (Toll road)
Yawkey
Cask 'n Flagon
BEERWORKS (No. 1 Boston/Fenway)
Lansdowne St
Restaurante especializado en fusión asiática Mei Mei
Park Dr
Buswell St
Buswell St
Iglesia bautista Ruggles Baptist Church
Arundel St
Maitland St
Restaurante mexicano Sol Azteca
Deerfield St

Figure 18. Path without Wi-Fi

In Figure 18, the user has walked the same path but without the Wi-Fi connection activated. As in the other images, the blue points are where the user walks in closed areas and the red ones are open areas.

First, it should be pointed out that most of the inappropriate jumps the track makes are located in the areas where the user is walking inside of a building. When walking inside the building, the application could not locate the phone, so it made some jumps between buildings, giving an approximate location of the user, sometimes correct and sometimes wrong. As in the previous case, a graphic of the distance error introduced by the GPS location, obtained by a comparison point to point, is shown (Figure 20).

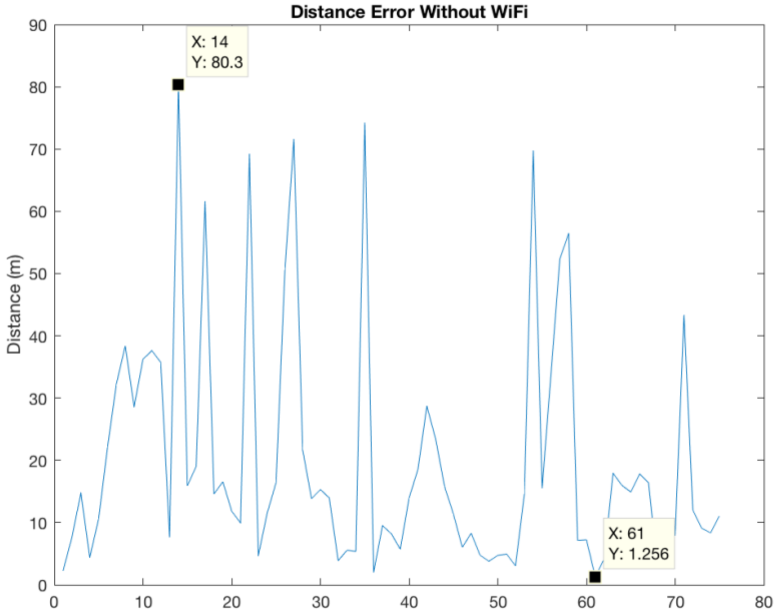


Figure 20. Distance Error without Wi-Fi

We see that here we have a higher number of points where the distance between the real point and the one obtained in the test is high. This is due to the fact that Wi-Fi helps establishing the correct position as the connection to the Wi-Fi router helps locate the phone in a smaller area, so it increases the precision. Therefore, it is a surprise that mean error in the distance is lower than in the case with Wi-Fi, being this mean error of 20.1 meters. In this case, the minimum error register is of 1.5 meters while the maximum is of 80.3 meters Also, most of the points are under 80 meters.

	With Wi-Fi	Without Wi-Fi
Minimum Error	8.358846725027389	1.2557
Maximum Error	200.1845927479665	80.3016
Mean distance error	73.574706798868960	20.0776

Table 2. Distance Error (m)

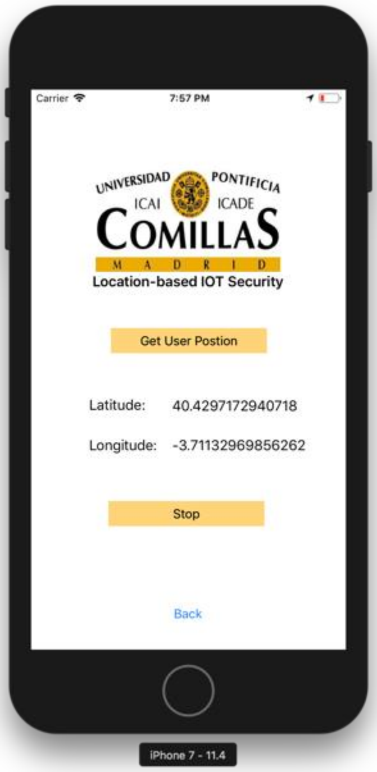
As another test, the Mean-squared error in both latitude and longitude for this path has been obtained. The MSE of the latitude for this case is of 3.8e-08 and in the case of the longitude is of 4.4e-08, being better in the case of the latitude, but with a smaller difference than in the case with Wi-Fi.

	With Wi-Fi	Without Wi-Fi
MSE Latitude	5.6302e-08	3.8635e-08
MSE Longitude	1.1157e-06	4.4544e-08

Table 3. MSE Coordinates

As an equivalent to this test, an app has been developed (Figure 21). This app captured the user's position every 5 seconds and displayed it on the user's phone. This proved that the position obtained by the GPS most of the timed changed, even though the user did not move.

This is caused by the error in precision mentioned before (in the case of the iPhone 60 meters most of the time). The user's coordinates changed in small amounts with each update of the position.



Latitude: 40.4297172940718

Longitude: -3.71132969856262

Figure 21. App Test User Position

5.3.2 GPS Delay Study

To study the time delay (or advancement) caused by the obtainment of the position by the GPS, as it is not constantly getting the position, I have profited from one feature provided by the reminders iOS app. This feature is: Remind Me when I arrive to a location. I have set a position and I have studied the time it took for the reminder to pop up. This time is either the time it will take to arrive to the location (and the distance to it) or time that the user has already been in the location. With this, I have recorded a number of occurrences in different scenarios. To generate the scenarios, I have recorded measures with the Wi-Fi on and off and using, or not using the Maps app.

The conclusion has been that, for the highest percentage of time, it did not matter which scenario the user was one, the reminder popped out two minutes after arriving to the destination. A table with a sample of the records is displayed (Table 2.).

When I arrive			
Distance to the location (m)	**Time (min)**	**Maps**	**Wi-Fi**
0	2:12	NO	YES
0	2:27	NO	NO
120	1:15	NO	YES
0	4:02	NO	YES
0	1:45	YES	YES
30	0:28	YES	NO
0	2:02	NO	YES
0	1:56	NO	NO
0	0:06	YES	YES
50	0:39	YES	NO

15	0:15	NO	NO
0	2:01	YES	YES
0	2:15	NO	YES
0	1:59	NO	NO
0	2:59	NO	NO
0	2:02	YES	NO
75	0:53	NO	YES
60	0:47	YES	YES
15	0:17	NO	NO
0	0:43	YES	YES
0	2:03	NO	YES
0	2:15	NO	YES
0	1:58	NO	YES
0	1:37	NO	YES
0	1:01	NO	NO
0	2:17	NO	YES
0	2:07	YES	YES
0	2:13	YES	NO

0	2:15	NO	NO
20	0:25	NO	NO
35	0:30	NO	NO
0	1:47	YES	YES
0	1:52	YES	YES
0	0:56	NO	YES
0	2:13	NO	YES
0	2:25	NO	YES
0	2:14	NO	YES
0	2:00	YES	YES
0	2:17	NO	YES
115	1:30	NO	NO
65	0:43	YES	NO
0	1:37	NO	NO
0	1:25	NO	NO
0	2:57	YES	YES
0	3:01	NO	YES
25	0:25	NO	YES

95	1:02	NO	NO
0	1:25	NO	YES
0	3:10	YES	YES
0	0:20	NO	YES

Table 4. Reminders Study

The final conclusion obtained from the previous studies is that, in order to reduce to the minimum both the false positives and the false negatives without compromising the system's security is establishing a radius of 60 meters. This radius is a bit over the assumed precision of the GPS but under the error mean for WiFi that the study showed. This is due to the fact this mean was affected by the outliers (both up and down) so it went higher than the radius that would be secure for this purpose. As the proposed system is going to be used in a closed area and the closed areas are where the effectiveness of the system went lower, the radius could not be smaller, as the false negatives would be too high, causing an effect similar to the Denial of Service (DoS) attack and would neglect the utility of the system.

5.4 STUDY TO IMPROVE PRECISION OF THE SYSTEM

For this part two different methods are analyzed to improve position accuracy. These two methods are the detection of the presence of the mobile phone via LTE packets and the use of a Beacon Bluetooth to improve the precision of the positioning of the user.

5.4.1 LTE DECODER

This method made use of Software Define Radio (SDR) to intercept information sent between the user and the cell tower. This method is based on the idea that, when a user walks inside a room, just for the simple action of carrying a mobile phone, which should be previously register as belonging to the user, the system detects it and identifies it as an authorized user.

The idea is to extract the TMSI number from the LTE packets. The TMSI (Temporary Mobile Subscriber Identity) is a unique identifier randomly assigned to the mobile and exchanged between it and the network. To extract this number, the USRP intercepts the paging packets. Meanwhile, the system starts sending different packets (calls, sms) so that the device will appear in the highest possible number of iterations, so the system could isolate the device and store the TMSI. We were not able to automatize this process, so it was tedious and required a high processing capacity.

With this method, once the system detected the phone, it automatically authenticated that user in the system. The problem is that it was implemented with the connection to a cell tower so, if the packets go through another tower they would not be detected. Also, the range of authentication in this project is really high and it was implemented only for one cell phone provider, as each one used a band range. When the user tried to authenticate, sometimes he would run into delays (sometimes to big), as a paging packet may not arrive, so the system would not authenticate him. This was solved by a manual authentication, which was just a simple button. This was not a safe second factor, as the button was access through the app, so the only necessary thing was to have the username and password.

This method, as explained, required a high level of processing, using at least a quad core, 8 GB RAM and 10 GB disk space computer. It also required the acquisition of a USRP B210 with an antenna supporting up to 5 GHz band, which is a pretty expensive device. The biggest issue of this project is that the TMSI, as indicated by the name, is temporary so it should be changed each time it changes. Also, depending on the telephone company, the range of frequencies vary. All this made this method unsuitable for the established purpose.

5.4.2 BLUETOOTH LOW ENERGY BEACON PRECISION

To improve the precision of the system and to reduce the delays described in 5.3.2, one of the possibilities that have been looked into is the use of a Bluetooth Low Energy (BLE) Beacon. The device being used is a Radius Networks RadBeacon Dot (proximity beacon) advertising with the iBeacon protocol (Apple's standard). This device has a variable radius of transmission that can be established by the user. It theoretically goes from 5 to 50 meters. Also, the advertising rate can be modified (100, 500 or 1000 ms). To establish the degree of improvement that should be experienced and the effectiveness of the Beacon in this project, the precision has been brought under the following tests: precision inside an apartment, precision in a detached house and precision in an open area. All these tests have been done thanks to a Radius Network application for the beacon called locate and other one called RadBeacon. These applications display all the Beacons nearby. Then, the user can look for their device and select it, so the application connects with it and starts receiving the information sent by the beacon (see Figure 22).

5.4.2.1 Apartment Test

The first test that has been done is to check the practical range of the Beacon in a flat of approximately 160 square meters. For the test, the Bluetooth has been located in the middle of the house with an established range of 12 meters. The mobile app was able to locate the user in most of the parts of the house, as they all were in the range, moving between 0 and 8 meters. The problem was when the device that tried to reach the Beacon was inside a bathroom, where the signal was lost. This may be caused by the material of the walls of the bathrooms, where wireless signals usually decrease. The marvel that usually covers the bathroom is a material that attenuates the signal [27][28]. The pipes that are providing water to the bathroom also work as a barrier for the wireless signal. The signal in the rest of the house was reachable and only experience signal loss outside the house. In the case the user was outside the house, if the door was open, the signal was still reachable but, if it was closed, it was not reachable from almost anywhere.

A different test was done in the same apartment. This time, the device was located in one end of the apartment. In this test, the other end of the house is on the edge of the range. Even though the device was set with a range of 12 meters, the app was able at some points to catch the signal when it was a bit over 12 meters. This only took place in areas where there were very few interferences and with door open. Most of the time, the signal was lost at 10 meters.

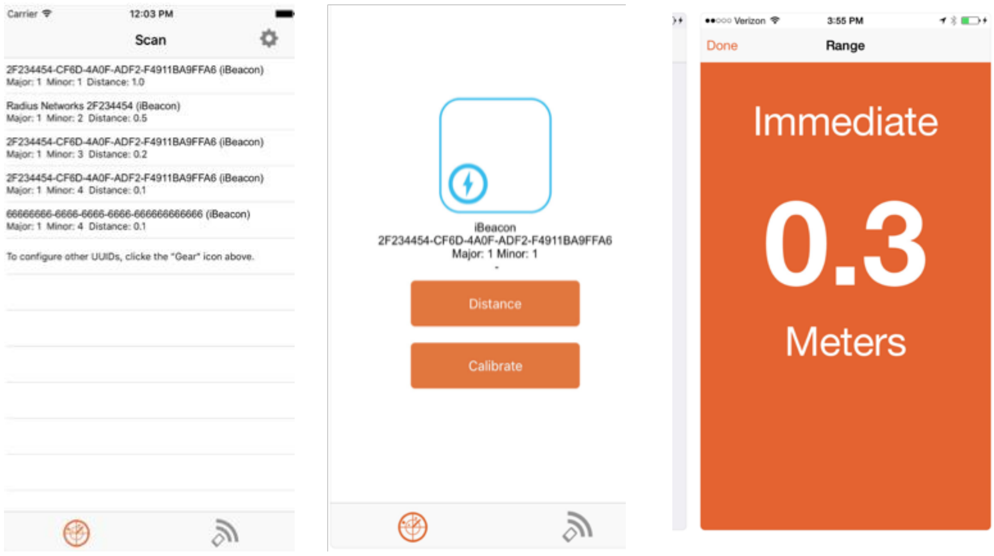
In a building, it has to be taken into account that, not only the materials of the house have an impact on the performance of the wireless device, but also all the wireless connections that the neighbors have. This may cause the performance of this precision enhancement method to deteriorate. On the other hand, it was proven that the effectiveness of the device to locate the user when he is inside the house is really high, making it a suitable method.

5.4.2.2 Detached House Test

First, clarify that the house where the measures were taken was a two-floor house. The range was left the same, as each floor was approximately of the same dimensions as the apartment were the previous test took place. When this test was made, the measures obtained around one floor were pretty similar to the previous test. In this case, the location of the Beacon (in meters) was a bit better, due to less interferences, which may be caused by the lower number of neighbor and them being further. A pro for the use of this method in detached houses is that the signal was well received in both floors, no matter in which one the device was. This is a pro for multiple floor houses but a con for flats, as the neighbors can receive and locate the beacon. The signal suffered the same changes due to materials in the detached house.

5.4.2.3 Open Area Test

This test was mainly performed to test the practical ratio of the devices. It was checked with the range set at both 12 meters and 50 meters. The test was performed in an open environment with almost nothing close to it. The surprising thing about this test was that the device, in some areas could go beyond the area of range (14.5 meters in the case of 12 and 53.9 in the case of 50) but in other case it did not catch the signal at way below the range (8.9 with 12 meters and 42 with 50 meters). The signal was also worst when the beacon was located in a higher point than the device, and there were walls of stone in between (these walls were low and did not cover the area).



2F234454-CF6D-4A0F-ADF2-F4911BA9FFA6 (iBeacon)
Major: 1 Minor: 1 Distance: 1.0

Radius Networks 2F234454 (iBeacon)
Major: 1 Minor: 2 Distance: 0.5

2F234454-CF6D-4A0F-ADF2-F4911BA9FFA6 (iBeacon)
Major: 1 Minor: 3 Distance: 0.2

2F234454-CF6D-4A0F-ADF2-F4911BA9FFA6 (iBeacon)
Major: 1 Minor: 4 Distance: 0.1

66666666-6666-6666-6666-666666666666 (iBeacon)
Major: 1 Minor: 4 Distance: 0.1

To configure other UUIDs, clicke the "Gear" icon above.

iBeacon
2F234454-CF6D-4A0F-ADF2-F4911BA9FFA6
Major: 1 Minor: 1
-

Immediate
0.3
Meters

Figure 22. Beacon App

Although this test proved that in an open area the signal was not always the expected, inside the two types of homes it worked in a reasonable precise way. In those two scenarios, the result was satisfactory so, in this test, it proved that the method is suitable to the project.

	Distance 12 m	Distance 50 m
	Practical Values (m)	Practical Values(m)
Minimum	8.9	42
Maximum	14.5	53.9

Table 5. Results Beacon Precision Study

Chapter 6. DEVELOPED SYSTEM

To implement the solution proposed in this project, an iOS app has been developed. This application makes use of the mobile phone's location services to establish the position of the user. This chapter is going to be used to provide a deeper explanation of the design of the system. Notice that a different application, from the one destined for the user has been created to help with the position tracking. It records regularly, every five seconds, the user position. This second application was shown before and it is not going to be explained here, as it is not a part of the main system that has been developed.

6.1 SYSTEM ANALYSIS

The proposed system makes use of an Apache server located on localhost. As a way to make it accessible and useful, it will have to be moved to an online cloud server. All the different data of the application has been stored in a MySQL database, that has been developed via Sequel Pro. The prototype mobile application works in an iOS operative system so the mobile devices that use it need to have this operative system. The application has been entirely designed making use of XCode and coded in Swift language. A similar app could be developed for other systems.

The app is connected to the server via HTTP connection. Because of this, as the users need to have connection to it, the system needs to be connected to the server through an internet connection and protected by means of a firewall (Figure 23).

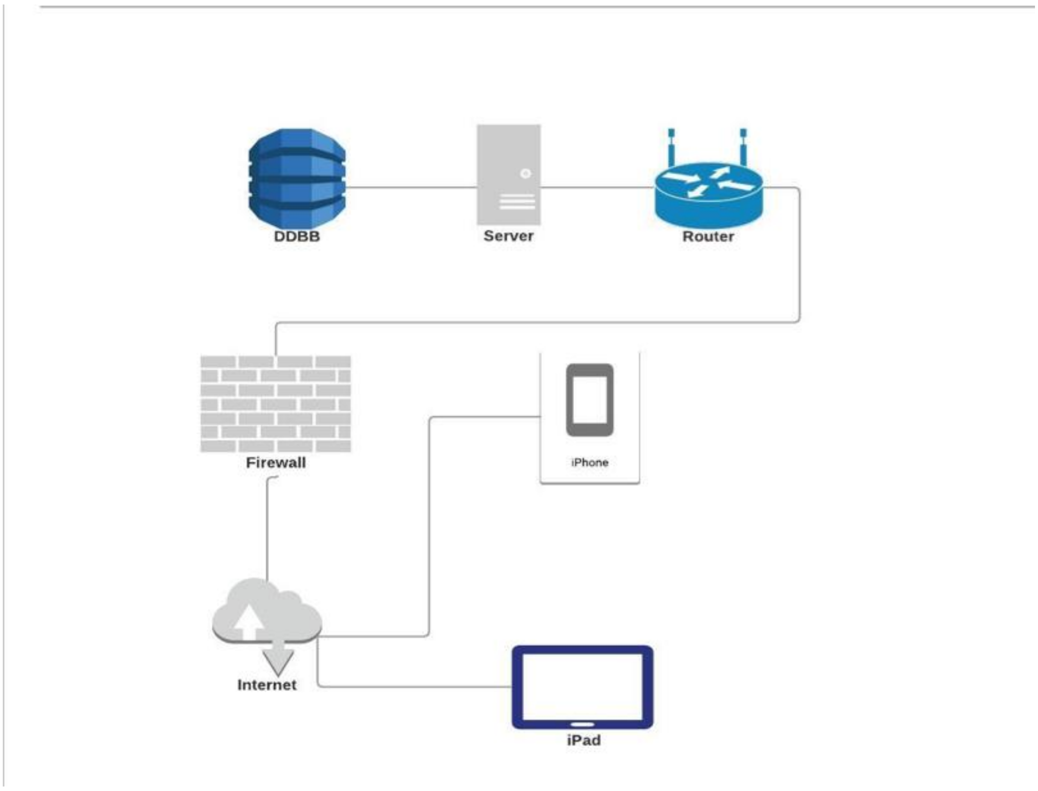


Figure 23. Architecture Diagram

6.1.1 DESIGN

This project follows a structure based on different modules. Each module controls a different functionality of the system independently. The modules are the following:

- User’s module
- Secure Locations Module
- IoT Authorization Module
- Command Manager

This is all connected as represented in the Block Diagram.

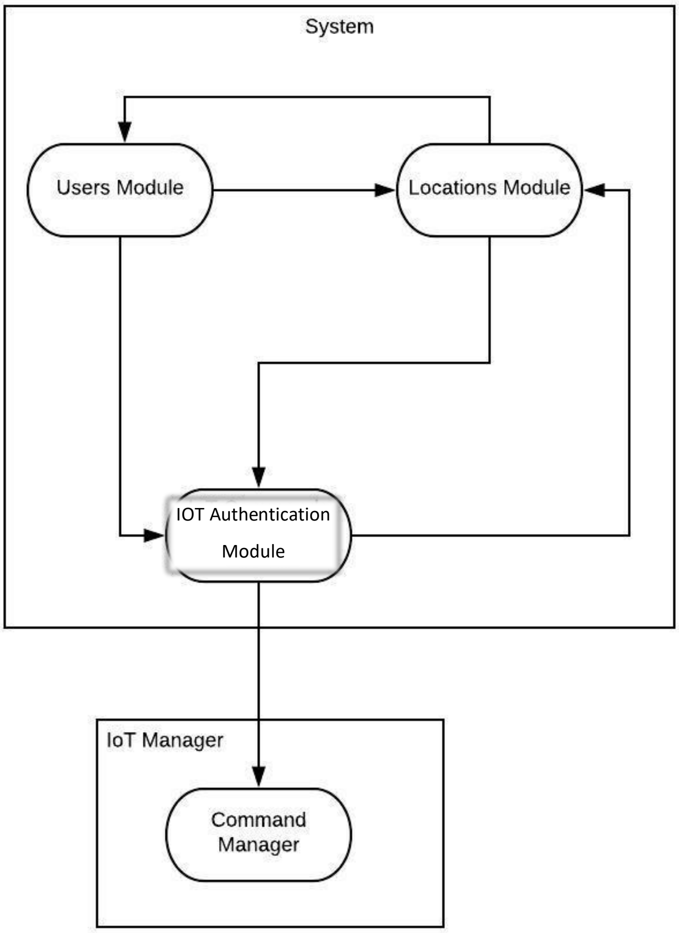


Figure 24. Blocks Diagram

6.1.2 USERS MODULE

In this module, all the information and processes related to the users are managed. This module includes the addition of new users. To create these new users, it requires all their information (Name, Surname, User Name, Email and Password). It classifies them via email (it cannot be repeated).

When the user starts using the mobile application, the first screen that appear belongs to this module. It is the first factor of authentication, the only one needed to authenticate the user to access the system. This module could present the following use cases:

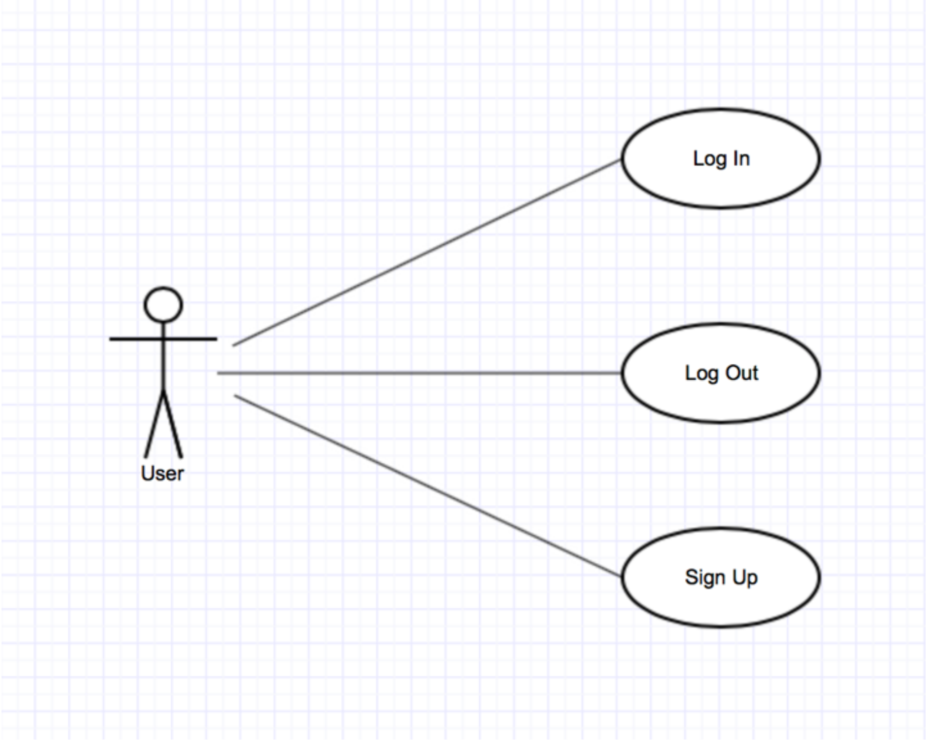


Figure 25. Use Case Users Module

6.1.3 LOCATIONS MODULE

In this module, all the information related to the Secure Locations of the users is managed. Also, all the actions that are performed involving the user position are managed in this module. Thanks to this module, the user can create a new secure location. In addition, the user will be able to delete or edit the locations he already has, as well as seen all the information about these locations. All these functionalities are shown in the next diagram:

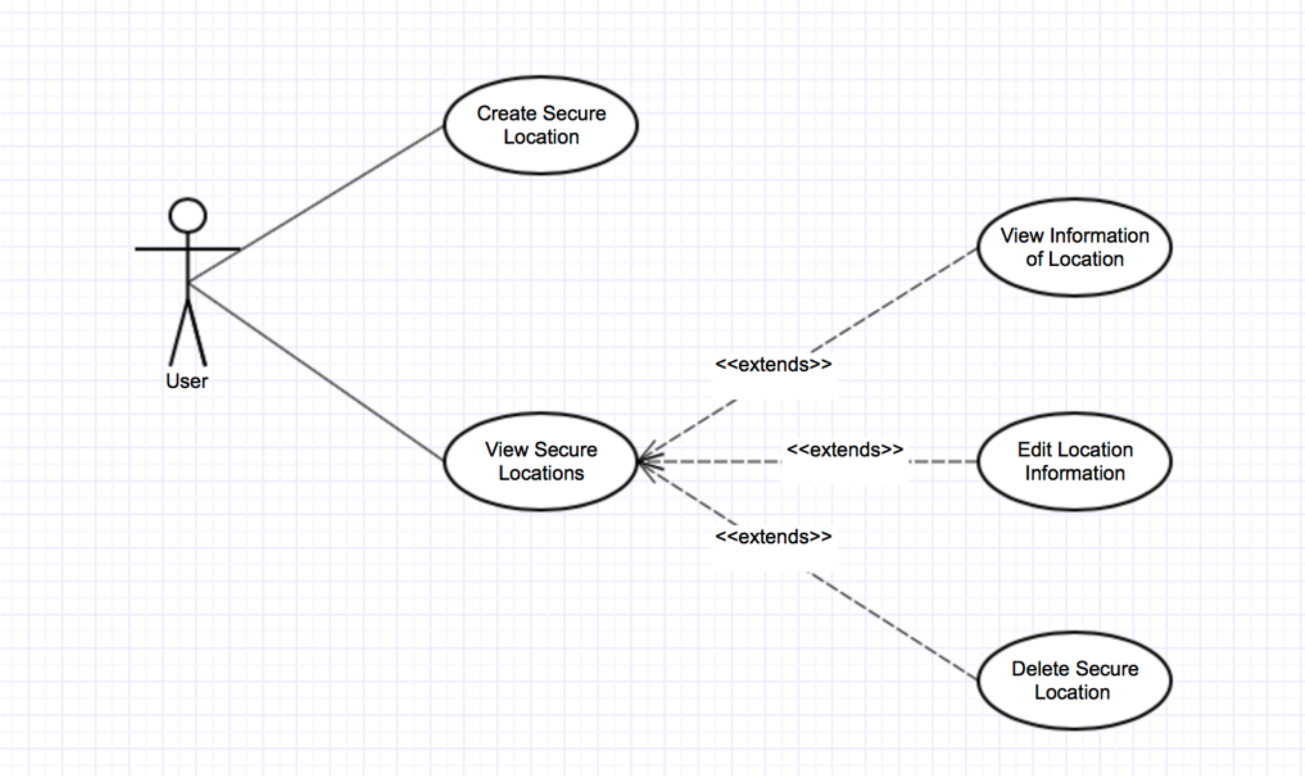


Figure 26. Use Case Locations Module

6.1.4 IoT Authorization Module

This module controls the IOT devices the user has, and it also sends the commands to the IoT devices. With it, the users can add new IoT. The user can also delete the devices he has. From every device, the user can select which action he wants to perform and send the command.

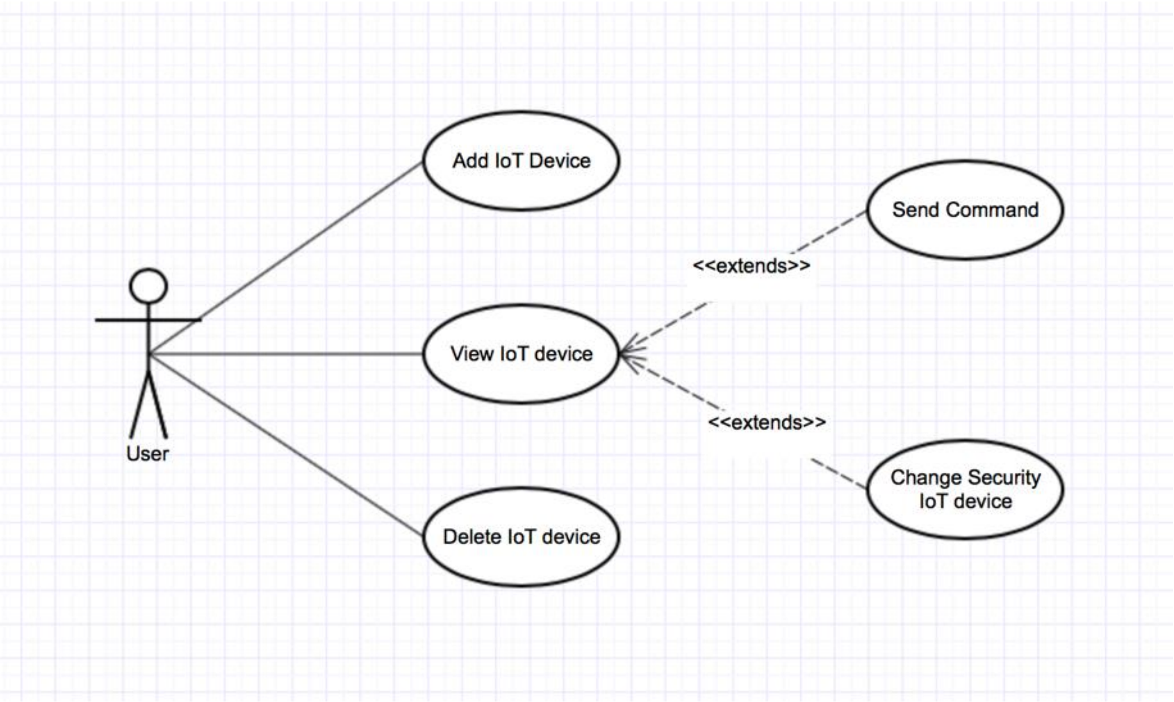


Figure 27. Use Case IoT Authorization Module

6.1.5 Command Manager Module

The last module is not part of the designed system. The proposed system acts only as an intermediate between the user's device and a platform that, once the system authenticates and authorizes the performance of the action, it sends the command to the physical device, so the action takes place. If the actions is risky, the system executes the second method of authentication and, if the user is in a secure location, it sends the external command manager the petition of command and the external system executes it.

6.2 IMPLEMENTATION

6.2.1 IOS

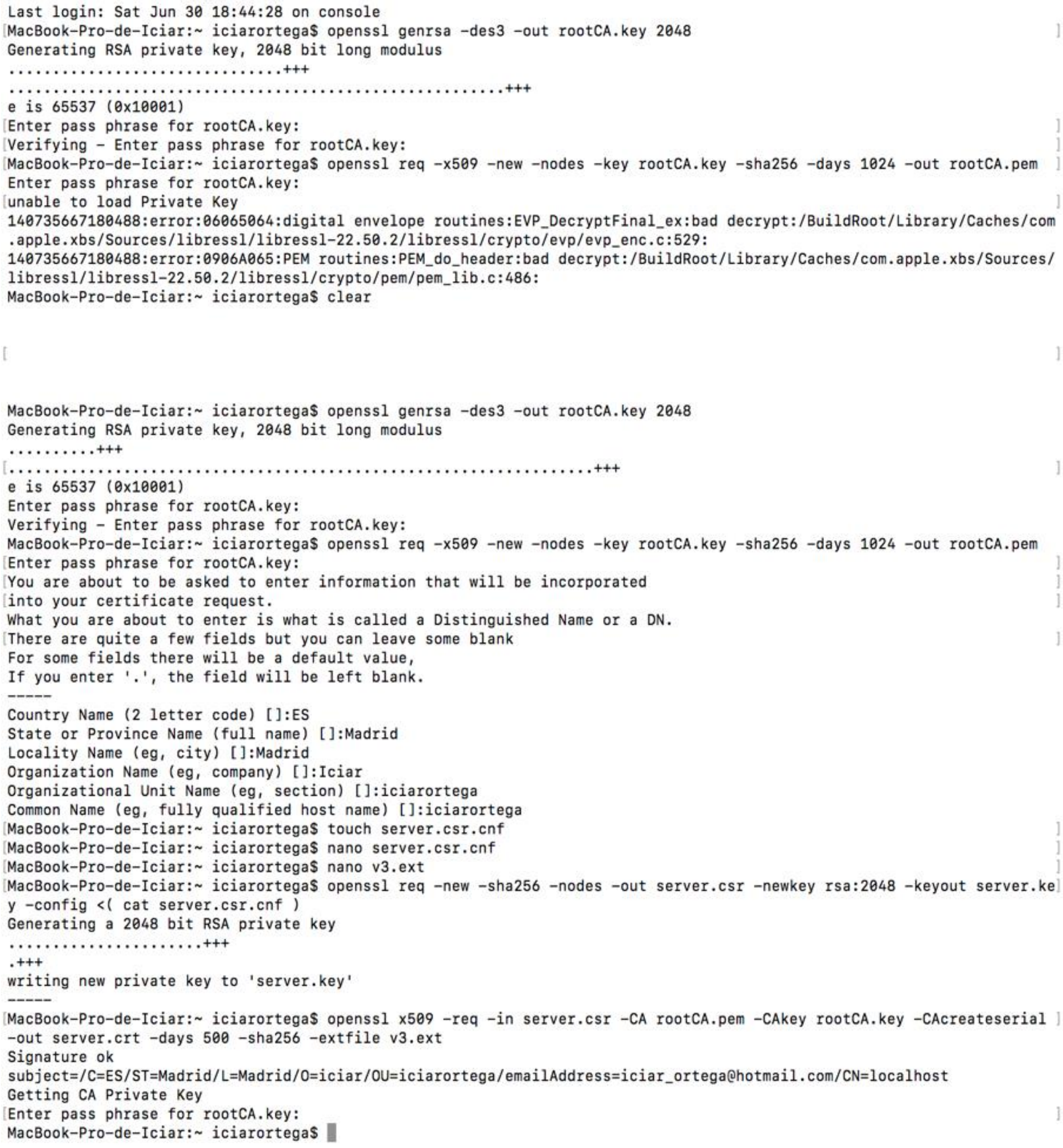
The prototype app for iOS needs to be able to obtain the position of the user through the mobile locations service to use it for the 2FA. Also, it needs to connect with the server that is the part of the system in charge of the authentication and the connection to the database. The connection between the server and the iOS app will be done through and HTTP connection.

6.2.1.1 Server Communication with App: HTTP and HTTPS

The client side of the system, the application, connects to the server via HTTP protocol. The iOS app connects to the server using POST and GET petitions. To be able to perform the mentioned connections, the app needs to use the *URLSession* class and related classes, classes that provide an API. The *URLSession* API provides a rich set of delegate methods for supporting authentication [29]. With the use of the API, the application is able to connect to the server via HTTP.

After selecting the class *URLSession*, the type of URL Session must be chosen. In this case, the connection is done using the singleton shared session, as the requests needed are simple and do not need big customizing of the session, but the use of a cookie is needed.

With iOS 9 came a new security feature, App Transport Security (ATS), which is enabled by default. This feature requires that all the HTTP connections are HTTPS. Hyper Text Transfer Protocol Secure (HTTPS) is a secure version of HTTP. With this, all the communications between the app and the server are encrypted. Even though there is a way around this in iOS, disabling the ATS for the specific server, the encryption in this project is desired. For the purpose of maintaining this, as the project was first developed with the server in *localhost*, came the need to enable the SSL. To do so, a Root Secure Sockets Layer (SSL) certificate was needed. First, I create an RSA-2048, which was inserted into a file. Then, the key is used to generate a Root SSL Certificate (Figure 28). As this certificate is a self-signed certificate, it is not trusted, so the preferences need to be changed to trust the certificate created by it. All this has to be done for the localhost to work. After this, a certificate is issued for the localhost [30]. This would not not need to be done in a real-life environment, as the certificate would not be self-signed, but the server should be able to be connected to via HTTPS. All the steps taken can be seen in Figure 28.



```
Last login: Sat Jun 30 18:44:28 on console
MacBook-Pro-de-Iciar:~ iciarortega$ openssl genrsa -des3 -out rootCA.key 2048
Generating RSA private key, 2048 bit long modulus
...............................+++
........................................................+++
e is 65537 (0x10001)
Enter pass phrase for rootCA.key:
Verifying - Enter pass phrase for rootCA.key:
MacBook-Pro-de-Iciar:~ iciarortega$ openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
Enter pass phrase for rootCA.key:
unable to load Private Key
140735667180488:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:/BuildRoot/Library/Caches/com
.apple.xbs/Sources/libressl/libressl-22.50.2/libressl/crypto/evp/evp_enc.c:529:
140735667180488:error:0906A065:PEM routines:PEM_do_header:bad decrypt:/BuildRoot/Library/Caches/com.apple.xbs/Sources/
libressl/libressl-22.50.2/libressl/crypto/pem/pem_lib.c:486:
MacBook-Pro-de-Iciar:~ iciarortega$ clear



MacBook-Pro-de-Iciar:~ iciarortega$ openssl genrsa -des3 -out rootCA.key 2048
Generating RSA private key, 2048 bit long modulus
..........+++
..................................................................+++
e is 65537 (0x10001)
Enter pass phrase for rootCA.key:
Verifying - Enter pass phrase for rootCA.key:
MacBook-Pro-de-Iciar:~ iciarortega$ openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
Enter pass phrase for rootCA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:ES
State or Province Name (full name) []:Madrid
Locality Name (eg, city) []:Madrid
Organization Name (eg, company) []:Iciar
Organizational Unit Name (eg, section) []:iciarortega
Common Name (eg, fully qualified host name) []:iciarortega
MacBook-Pro-de-Iciar:~ iciarortega$ touch server.csr.cnf
MacBook-Pro-de-Iciar:~ iciarortega$ nano server.csr.cnf
MacBook-Pro-de-Iciar:~ iciarortega$ nano v3.ext
MacBook-Pro-de-Iciar:~ iciarortega$ openssl req -new -sha256 -nodes -out server.csr -newkey rsa:2048 -keyout server.ke
y -config <( cat server.csr.cnf )
Generating a 2048 bit RSA private key
......................+++
.+++
writing new private key to 'server.key'
-----
MacBook-Pro-de-Iciar:~ iciarortega$ openssl x509 -req -in server.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial
-out server.crt -days 500 -sha256 -extfile v3.ext
Signature ok
subject=/C=ES/ST=Madrid/L=Madrid/O=iciar/OU=iciarortega/emailAddress=iciar_ortega@hotmail.com/CN=localhost
Getting CA Private Key
Enter pass phrase for rootCA.key:
MacBook-Pro-de-Iciar:~ iciarortega$ █
```

Figure 28. Enable HTTPS in localhost

This self-signed certificate had to be also accepted on the testing device as it is not a known and authorized certificate. In a commercial environment, the server should be using a certification signed by a Certification Authority (CA) and the application or phone will not need to stablish the trust manually, as the certificate would be recognized.

6.2.1.2 JSON

JSON is a light text format that is used for the exchange of data. It is being used for the exchange of information between the server and the application. The information has been serialized in the server for its easy transmission.

Before sending the information, the following function has been implemented.

```
            json_encode($user_devices);
```

Then, in the app, this information has to be deserialized.

6.2.2 USERS MODULE

Following, a description of the processes that take place in this module is going to be displayed.

6.2.2.1 New User (Sign Up)

To be able to start using the application, the user needs to sign up in the system. In this sign up, the server randomly generates a cookie that is assigned to that user and stored. This cookie is sent in all the log in requests, along with the user's information, to uniquely identify the user, as an addition of security.

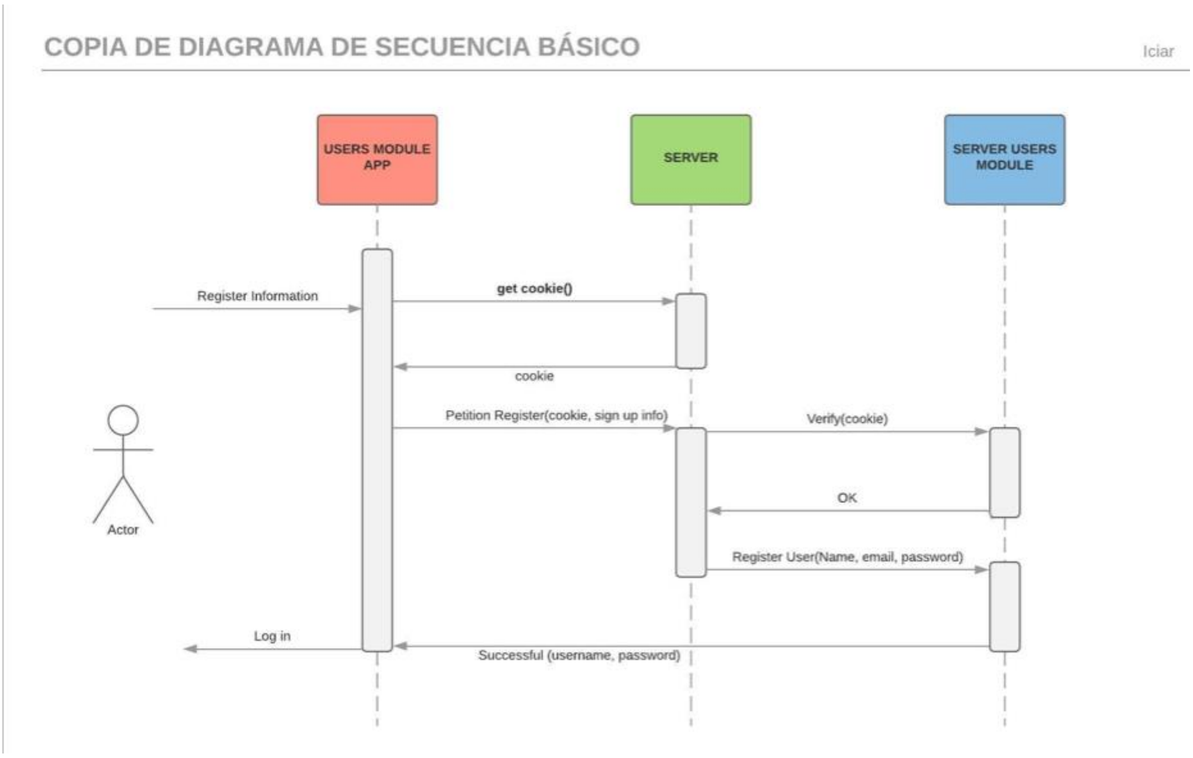

COPIA DE DIAGRAMA DE SECUENCIA BÁSICO
Iciar
USERS MODULE APP
SERVER
SERVER USERS MODULE
Register Information
get cookie()
cookie
Petition Register(cookie, sign up info)
Verify(cookie)
OK
Register User(Name, email, password)
Actor
Log in
Successful (username, password)

Figure 29. Sequence Diagram Sign Up

6.2.2.2 Log Out

When the user wants to log out, can do it from any point in the application just clicking on the button located at in the bottom of the view. When clicking, the user is sent back to the log in page.

6.2.2.3 Log In

When the user logs in the mobile application, he has to insert the login information. When he tries to send it, the app automatically inserts the cookie in the message and then sends it. The server checks whether all that information is correct and the sends back an authorization for the user, who is then able to enter the application and use it.

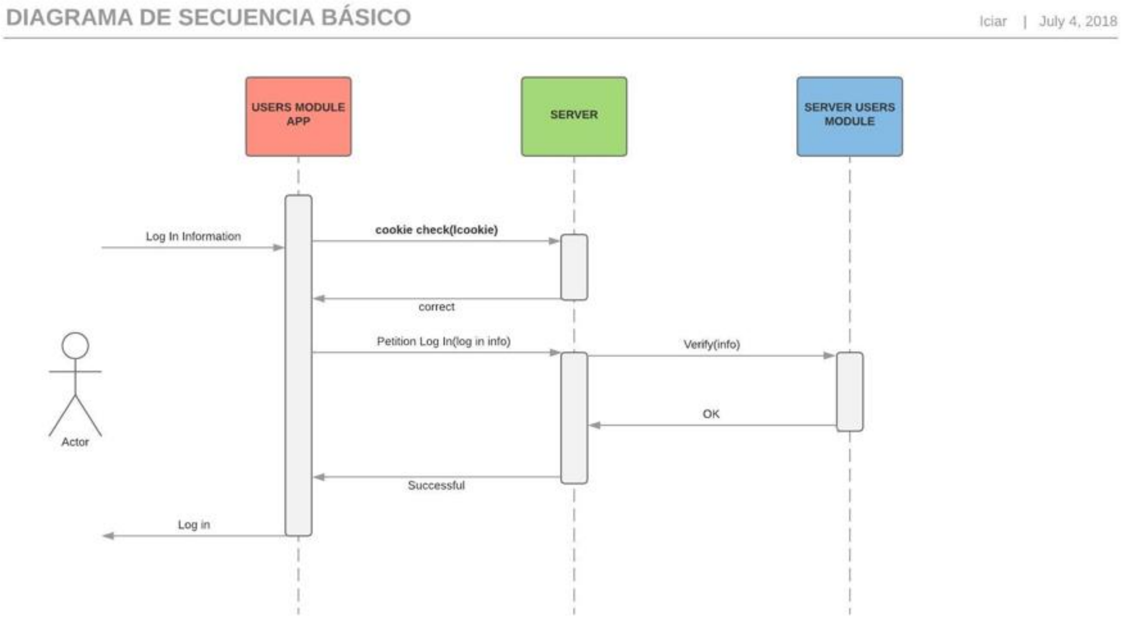


Figure 30. Secuence Diagram Log In

6.2.3 LOCATIONS MODULE

When the user gets into the app, he can either go to the Locations Module or to the IoT authorizations module. If the user accesses the locations module he can see the locations he already has register, edit those locations, delete them or add a new secure location. The management of the secure locations is done from both: *SecureLocationsViewController.swift* and *ManageSecureLocationsViewController.swift*, that are connected to each other. In the *SecureLocationsViewController.swift* the user can create new secure locations.

6.2.3.1 Add new Location

To start getting the location, when the view is loaded, the following is created:

```
    var locationManager: CLLocationManager!

    override func viewDidLoad() {
        super.viewDidLoad()

        locationManager = CLLocationManager()
        locationManager.delegate = self
        locationManager.desiredAccuracy = kCLLocationAccuracyBest
        locationManager.requestAlwaysAuthorization()
        locationManager.startUpdatingLocation()

    }
```

With the *requestAlwaysAuthorization(),* the applications ask the user for permission to start using his position. Then, the user coordinates are obtained as follows:

```
func locationManager(_ manager: CLLocationManager, didUpdateLocations locations:
[CLLocation]) {
        let userLocation: CLLocation = locations[0] as CLLocation

        let latitude = userLocation.coordinate.latitude
        let longitude = userLocation.coordinate.longitude

        latitudeString = String(latitude)
        longitudeString = String(longitude)
    }


    func locationManager(_ manager: CLLocationManager, didFailWithError error:
Error) {
        print("Error \(error)")
    }
```

To be able to use the position, MapKit should be imported.

```
    import MapKit
```

This position is then sent to the server, which compares it with the other locations the user has and, if it is not created yet, it adds this new position.

6.2.3.2 Manage Locations

The app sends an HTTP request to the server to get the locations that the user has. The HTTP request is done as shown below.

```
let UserSecLoc = URL(string: "https://localhost/ManageLocations.php")

        var request = URLRequest(url: UserSecLoc!)

        request.httpMethod = "POST"

        var info = ""
        info = "Email="+email!+"&Password="+password!

        request.httpBody = info.data(using: .ascii)


        let SecLocTask = URLSession.shared.dataTask(with: request){ (data: Data?,
response: URLResponse?, error: Error?) in

        }

        SecLocTask.resume()
```

Once this call is done, the server obtains the locations and, using JSON, it sends them back to the app. The app then has to parse it and serialize it to be able to display it later.

```
             let path = Bundle.main.path(forResource: "json", ofType: "json")
                do {
                    let jsonData = try Data(contentsOfFile: path!)
                    guard let parsedJson = try JSONSerialization.jsonObject(with:
                    jsonData) as? [String:Any]
                        else {}
                    guard let locations = parsedJson["locations"] as?
                    [[String:Any]]
                        else{}
                    print(locations)
                } catch {
                    print(error)
                }
```

6.2.4 IoT Authorizations module

This module enables the user to view which IOT devices he has registered and edit this information (add or delete devices). Also, if the user selects one device, the user is redirected to the display page of that device, in where he can see which actions the device can perform.

To perform these actions, as in the previously exposed module, the iOS application connects to the server through an HTTPS connection which connects to the database to extract the information and sends it back to the mobile application with JSON. This information is the displayed by the app.

6.2.5 Command Manager Module

This module is external to this prototype. It should to be developed in the future. This module's goal is to interact with the proposed system and interpret the authorization sent by the server to perform the action selected by the user. This module only has to send the command as, if the user is not authorized to perform the action, no information or command would be sent to this module.

6.2.6 Database Structure

The database counts with four tables:

- USERS table: this table holds the information about the user. The components of the table are the user name, surname, username, email, password (stored saving the hash that is obtained using SHA512 and a salt) and a cookie.
- DEVICES table: the user identifier (email in this case) and the devices he has register.

- ACTIONS table: it stores the different devices that are controlled by the system, the actions that the devices can perform and the level of risk of the action (risky and not risky)
- SECURE LOCATIONS table: it stores the identification of the devices (email), the latitude, longitude and the name of the Location.

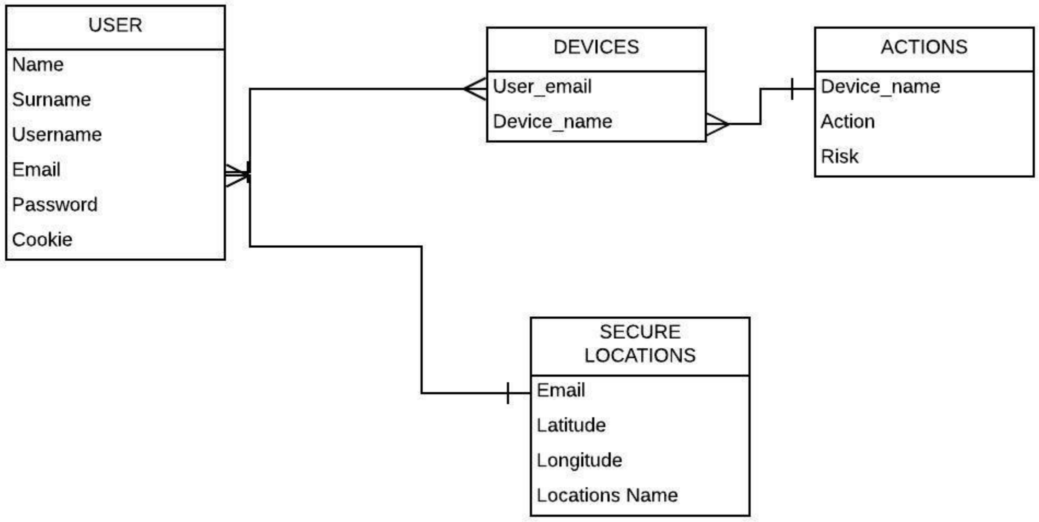


Figure 31. Classes Diagram

6.2.7 SERVER SIDE

As mentioned before, the server has been coded using PHP. This server is currently located on the localhost of the computer where all the system is being developed. If this system was available to the users, it should be located on a cloud server. The server mainly works as an intermediary between the database and the applications although it performs the most important function of the project: it checks if the users are located inside the radio of any of their secure locations. The tasks of the server are:

- Inserting a new user into the database after generating a unique cookie to identify the user

- Check if the log in data is correct
- Add, remove and obtain the secure locations of the user
- Compare the location of the user to the radius around the locations that he has stored as secure.
- Add, remove and obtain the IOT devices of the users, along with their capacities and the level of risk
- Send approval of disapproval if the user is in a secure location

The main, most important task of the server is the part involving the second factor authentication. In Figure 32, there is an activity diagram representing how this works.

In order to do this, the server first check if the action is listed as risky.

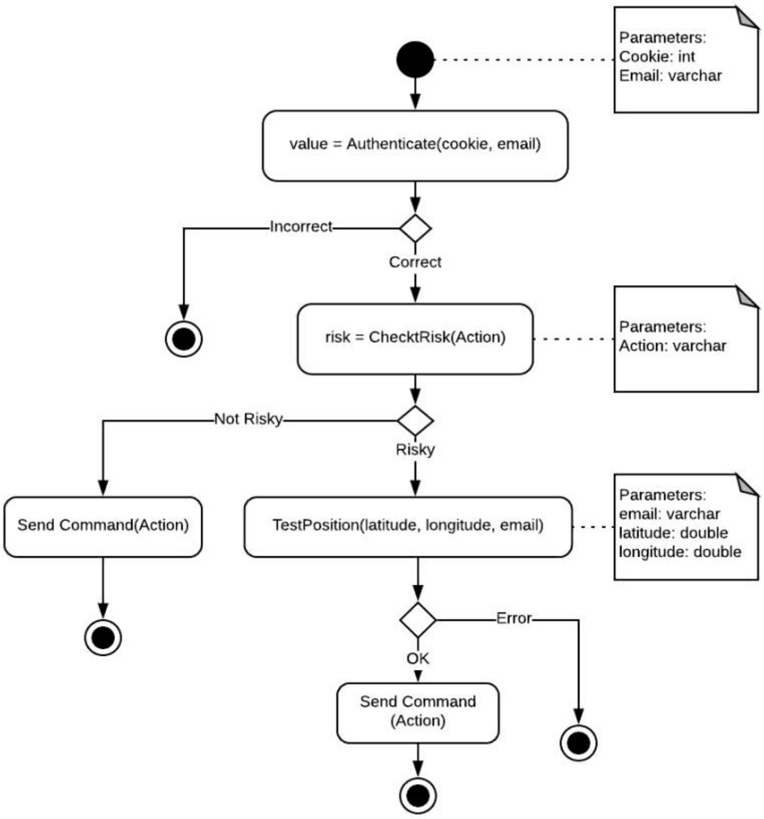


Figure 32. 2FA Activity Diagram

```
try{

        $sql2 = "SELECT Risk FROM ACTIONS WHERE Action ='$action'";

        foreach ($conn->query($sql2) as $row ){
                $int_risk = $row['Risk'];
        }
}catch(SQLException $eSQL){
        echo "SQL Error: \n" . $eSQL->getMessage() . "\n";
}
```

If the answer to this is that the action is risky, it then checks the position of the user and compares it to the secure locations:

```
                $sql = "SELECT Latitude, Longitude FROM SECURELOCATIONS WHERE
        email='$email'";

                foreach ($conn->query($sql) as $row ){

                $dist= distance($latitude, $longitude,
        $row['Latitude'], $row['Longitude']);
```

If it is inside of any of the radius around the secure locations (<60 meters), the server will send the command. If it is not, an error message will be displayed on the user's phone. More information about this will be explained in the next chapter.

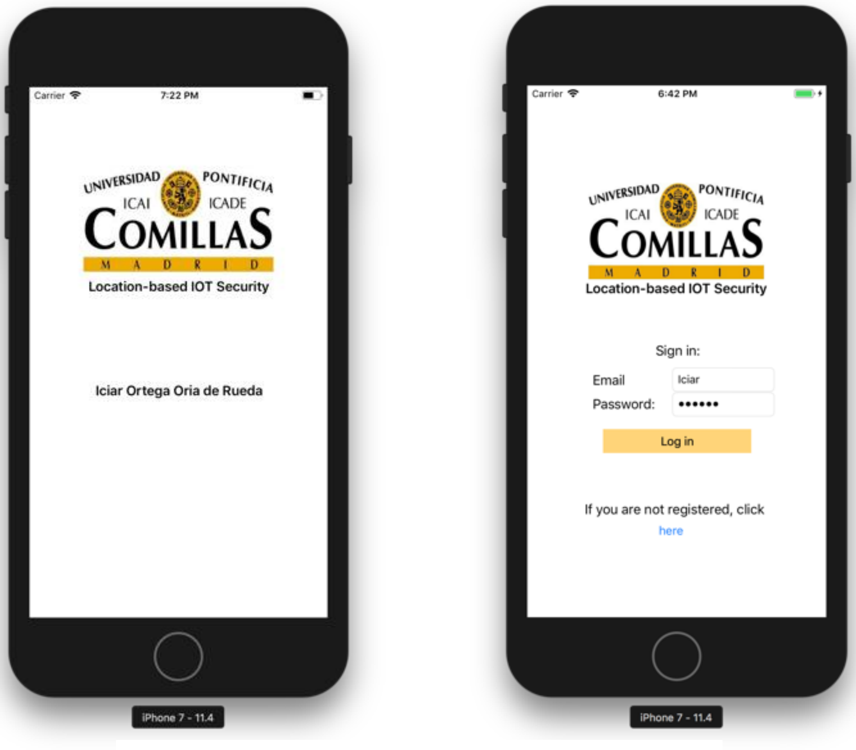
Chapter 7. RESULTS ANALYSIS

This chapter shows the results and system obtained from the previous chapters (Chapter 5. and Chapter 6.).

7.1 MOBILE APPLICATION

7.1.1 LOGIN PAGE

When the user opens the mobile application, after the loading page, the login page opens up. This page is coded and controlled by *DataViewController.swift.* If the user has already created an account, he can introduce his email and his password to access the system. If not, the user has to click the button *here* to get to the register page.



Location-based IOT Security

Iciar Ortega Oria de Rueda

Location-based IOT Security

Sign in:

Email: Iciar

Password: ••••••

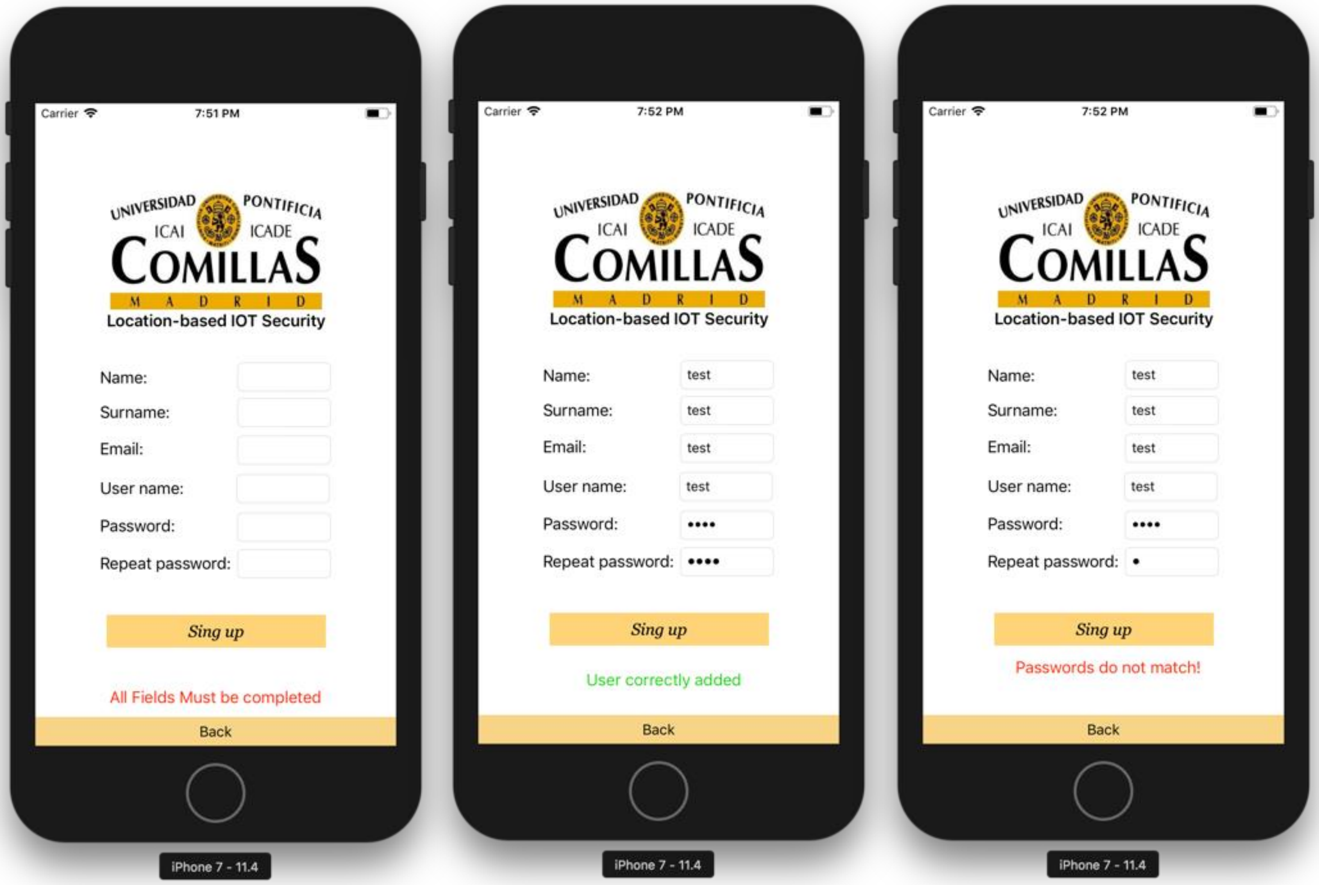
If you are not registered, click here

Carrier
7:22 PM
UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID
iPhone 7 - 11.4
Carrier
6:42 PM
UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID
Log in
here
iPhone 7 - 11.4

Figure 33. Loading Page and Log in Page

7.1.2 SIGN UP PAGE

As mentioned before, if the user has not created an account, he could do so by means of the sign-up page. The user has to introduce all his information and then, click the button to register. If the user does not complete al the fields, an error will appear, as well as if the passwords do not match. If the user is correctly inserted, it will be announced and signed in. This page is controlled by the *SignUpViewController.swift*.



Carrier 7:51 PM
Location-based IOT Security
Name:
Surname:
Email:
User name:
Password:
Repeat password:
Sing up
All Fields Must be completed
Back
iPhone 7 - 11.4

Carrier 7:52 PM
Location-based IOT Security
Name: test
Surname: test
Email: test
User name: test
Password: ••••
Repeat password: ••••
Sing up
User correctly added
Back
iPhone 7 - 11.4

Carrier 7:52 PM
Location-based IOT Security
Name: test
Surname: test
Email: test
User name: test
Password: ••••
Repeat password: •
Sing up
Passwords do not match!
Back
iPhone 7 - 11.4

Figure 34. Sign up page: Empty fields, Correctly inserted, Password Mismatch

7.1.3 MENU PAGE

As an intermediate page, the user will get to the menu. From there, he can move around all the different features of the mobile application. This page is controlled by the *IntermediateViewController.swift* file.

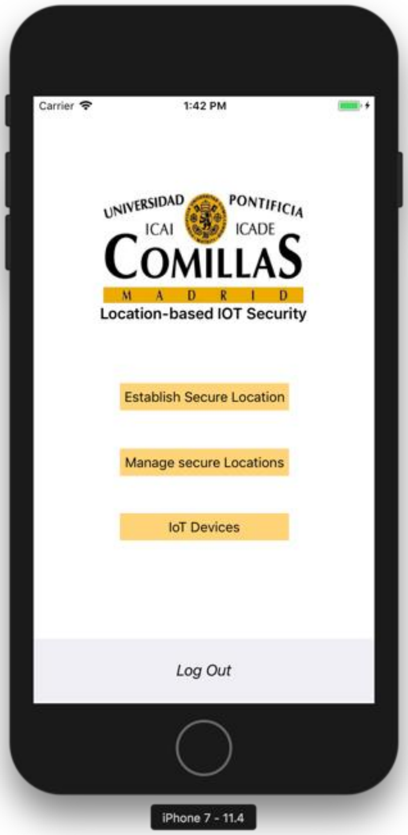


Figure 35. App Menu

7.1.4 ESTABLISH SECURE LOCATION

When the user clicks on the Establish Secure Location on the menu, he gets redirected to the following page. In this page, the user can create a new Secure Location. The user is prompted with a map where his position is shown. There is a text field where the user has to name the new secure location. After this, the user has to click on Establish this position as secure and, if he is already are in a secure area and the one they are trying to introduce does not exist on their profile, or it is the first area he is adding, this area will be added to his information. This is controlled by the *SecureLocationViewController.swift* file.

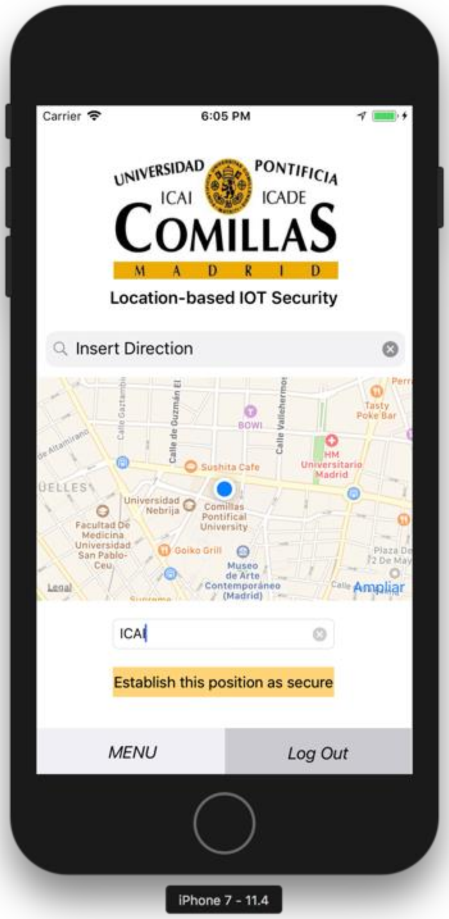

Carrier
6:05 PM
UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID
Location-based IOT Security
Insert Direction
Sushita Cafe
Universidad Nebrija
Comillas Pontifical University
Goiko Grill
Museo de Arte Contemporáneo (Madrid)
HM Universitario Madrid
Tasty Poke Bar
Ampliar
Legal
ICAI
Establish this position as secure
MENU
Log Out
iPhone 7 - 11.4

Figure 36. Creation of Secure Locations

7.1.5 MANAGE SECURE LOCATIONS

In this page, the user can see all the places that he has established as secure. From here, he can delete the location or click on the ⊕ button to add a new location. If the user clicks that button, he will be redirect to the Establish Secure Location page. There is also a bar where the user can click to go back to the Menu page or log out. This view is controlled by *ManageSecureLocationsViewController.swift* file.

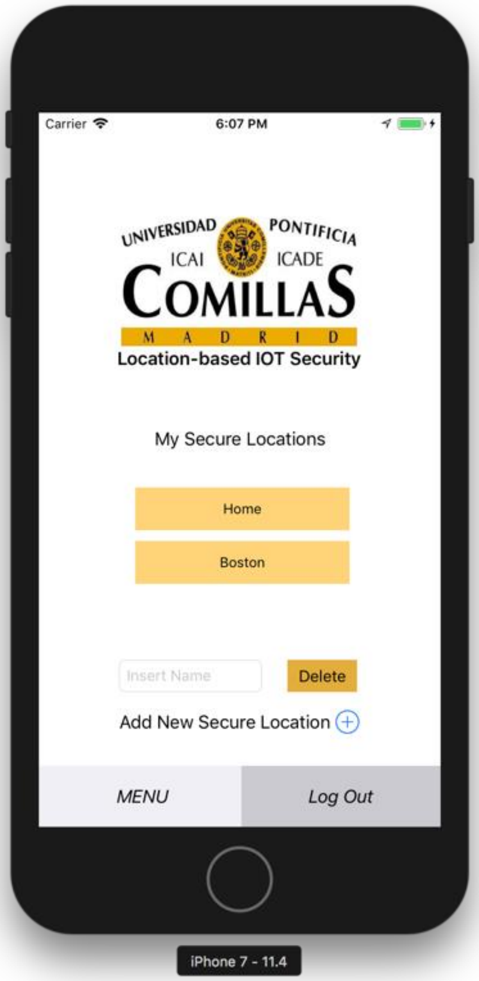

Carrier
6:07 PM
UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID
Location-based IOT Security
My Secure Locations
Home
Boston
Insert Name
Delete
Add New Secure Location ⊕
MENU
Log Out
iPhone 7 - 11.4

Figure 37. Manage Secure Locations

7.1.6 SEE AVAILABLE IOT DEVICE

In this page, the user can see what IoT devices he has and access the device by clicking on the view button. To add new devices, the user will have to click on the add button. By clicking this button, he will be redirected to the corresponding device page. The displayed page is controlled by the file *DisplayDeviceViewController.swift.* As in all of the pages, the user can both go to the menu and log out.

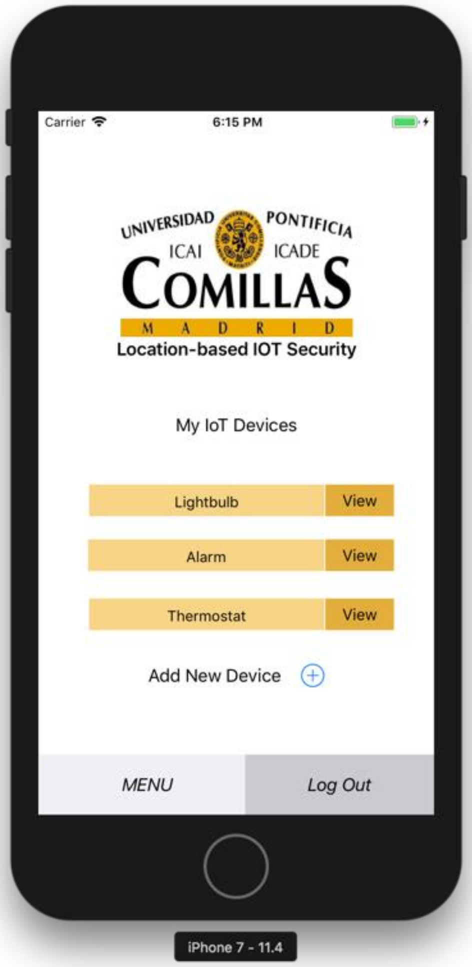
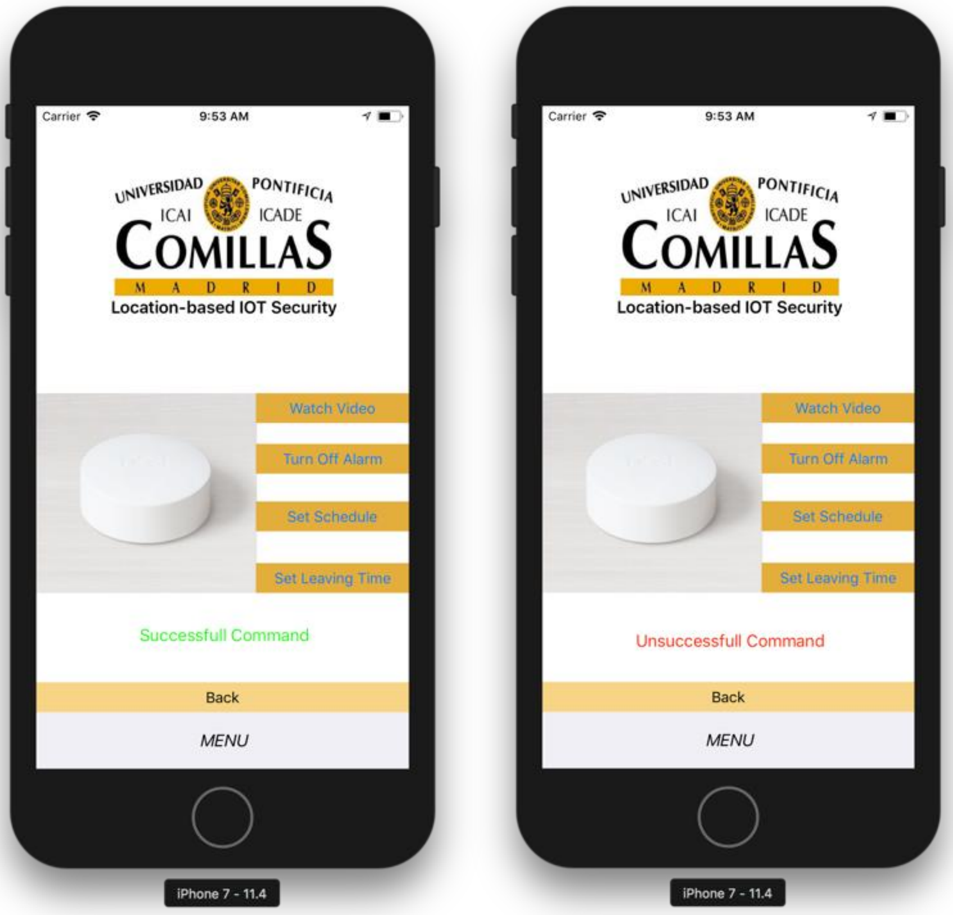


Figure 38. Available devices Control Page

7.1.7 IoT Device Control Page. 2FA Authentication

Once the app user has selected a device, a new page appears with the selected device and the appropriate actions that he could perform. By clicking in any of this actions, the process of 2FA will start. From this page, the user can also delete the device.



Successfull Command

Unsuccessfull Command

Figure 39. Control of IoT devices Page

To do the authentication tasks, the app gathers the information about the position of the user (latitude and longitude) and sends the request to the server. The query to the server has to include the following information:

- Latitude and longitude: the coordinates of the position of the user
- Email: email of the user sending the command
- Action: name of the action that the user wants to perform
- Cookie: the cookie that uniquely identifies that user

The information will look like this:

```
info = "Latitude="+latitudeString+"&Longitude="+longitudeString+
"&Email="+email!+"&Action="+action!+"&Email="+email!+"&Cookie="+ cookie!
```

And then, this will be sent to the server through HTTPS. This data is inserted in the HTTPS petition as follows:

```
request.httpBody = info.data(using: .utf16)
```

If the action is not considered risky, the server discards the information about the position and automatically sends the command (currently it only notifies that the command was successful). If it is considered risky, the server checks the position of the user and checks if it is located in a radius under 60 meters around any of the user's secure locations. If it is, it will try performing the command, if not, the user will receive a message saying that the command was unsuccessful. The Diagram of Action describing this is shown in Figure 40.

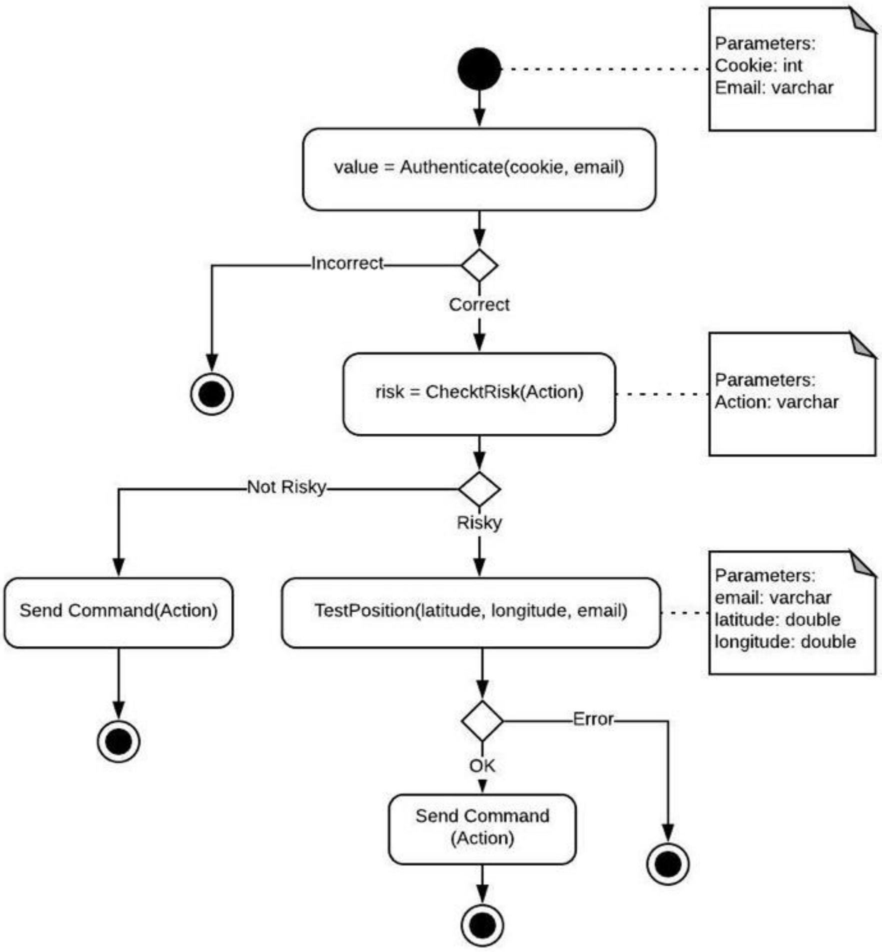


Figure 40. Authentication Activity Diagram

There should be a concern about “Replay Attacks”. In this kind of attacks, it is possible to repeat a request several times, even if the request is encrypted and the attacker doesn’t know the contests of the message. For example, if the users send a message to lower the temperature one degree, and the attacker replays that message several times, then the temperature will end up in the minimum setting value. However, using HTTPS protocol this threat is largely mitigated.

HTTPS protocol is an extension of HTTP that uses TLS (Transport Layer Security) to encrypt the data. It is considered secure for preventing Replay Attacks because of the way in which TLS is implemented, because it uses a new set of keys for each connection and assigns a unique sequence number to each record. Only in exceptional cases with the attacker in a privileged network position could potentially Replay a request [31].

The possible combinations and corresponding outcomes of this authentication are displayed in the Table 6. Where there is a ✓ it means that the action in enabled and performed. Where there is a ✗ it means that the action would not be performed, as the user would not be authenticated.

Location / Action	Unsecure	Secure
Risky	✗	✓
Non-Risky	✓	✓

Table 6. Posible Outcomes of Authorization

7.2 SERVER

The server-side has a similar structure in all of its functions. In all of them, a connection to the database has been made to retrieve the information. This information could be to authenticate the user's login, to get its secure locations, its devices or the functions and level of risk of these devices. The communication to the database and the commands to interact with it are describe below. To open the communication with the database and establish how it should be done, the server is designed as follows:

```
$conn = new PDO("mysql:host=$servername;dbname=locationUsers", $username,
$password);

       $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
```

After this, depending on the action that wants to be performed, the SQL statement varies. The processing of the answer varies depending on the statement. An example of how these statements look like is the next one:

```
$sql = "SELECT Latitude, Longitude FROM SECURELOCATIONS WHERE email='$email'";
```

The most important function of the server is to determine whether the position of the user is secure or not, even if it is not in the exact location establish as secure. It has to check if the user is located inside the radius around the secure location. For this, the following function has been implemented to establish the distance from the secure locations to the point where the user is. This process is done for all the locations and, if the distance to any of the positions is inferior to the established radius (60 meters), the user is authorized and enabled to perform the desired action, sending in the future the command to the IoT device through and intermediate system. The function developed in the server for this comparison is the following one:

```
       function distance($lat1, $lon1, $lat2, $lon2) {

         $theta = $lon1 - $lon2;
         $dist = sin(deg2rad($lat1)) * sin(deg2rad($lat2)) +  cos(deg2rad($lat1))
* cos(deg2rad($lat2)) * cos(deg2rad($theta));
         $dist = acos($dist);
         $dist = rad2deg($dist);

         $distan = $dist * 60 * 1.1515 * 1.609344;


         return $distan;

       }
```

Then, this distance is compared to the radius and, if it is under it, an authorization message is sent.

7.3 ANALYSIS

As far as the system goes, the analysis is positive. Most of the goals of this system were theoretical. There was a need to perform different studies to establish the viability of the project and the trustworthiness of the technologies intervening in the security process. Although the lines that need to be established are a bit blurry and subjective, the studies have proven this system to be useful.

In terms of system, the goals that influenced it were:

i. Development of a mobile application to determine the position of the user and analyze the precision of this location.
ii. Present the concept of secure location and establish them. Implement the web-server application to manage actions.

The first point required the design of an application to analyze the precision of the system. This goal was achieved and proved to be useful, but it is not included in the final system, as it was only for the testing shake, having no utility for the user.

The second point resulted on the explained system. The result is positive, as the app is able to get the user position and send it along with the action request. The server receives the request and it the information on the command is used to extract the location, analyze it and discriminate if the location is secure or not and communicate it to the user. In the future, it should send the indication to the intermediate module to perform the action, instead of communicating it to the user. An error on the authentication would still be communicated in future developments.

Chapter 8. CONCLUSIONS AND FUTURE PROJECTS

Although it may be difficult to draw a line between risky and not risky actions, even more if it is done trying to have the least impact in the functionality of the devices, it can be done. The proposed system provides an extra layer of security to the actions that may cause the biggest harm to a user's home. It also has to be taking in to account that not only those actions that could cause damage on the user's home should be protected. Also, it has to be analyzed which devices and with which actions reveal the most about the user, as IoT devices have been proven to be a good source to obtain user's behavior, which is an invasion of their privacy and a breach of information.

In the digital world we live in, Internet of Things devices will do nothing but grow even more. The security of these devices should be our main concern, as these devices know our patterns and our activities. They hold very important information about users' life. Users are not always aware of the damages an attack on these devices can cause. This results in a lack of concern about security that does not work well with adding up more security layers for the user to handle. This project is really important and adequate, as it protects the user, but it is not seen as an obstacle, as it is done in the background with hardly any intervention of the user (just establishing the secure locations).

As studied, GPS precision in closed areas decreases and it is not able to accurately locate the user inside a building. As this project is destined for closed areas, to prevent the false negatives due to this lack of precision, a radius has been stablished. For this, also it has been taking into account that false positives should be minimum. The result has been a radius of 60 meters. This radius may be considered really big if the project aims not only to protect from any attacker but also from people in the user's area. This is an area that should be worked on, searching for new methods of position that are available in most locations. The enhancement of the Beacon is convenient, especially for home as it should be the most common location

This project is currently user oriented. By this, I mean that it is mainly destined to be used to protect the user's home assets. In the future, I think this project should try to be oriented to the industry world, as nowadays the number of intelligent devices being used in this sector is humongous.

8.1 FUTURE WORK AND IMPROVEMENTS

Once all the studies have been made and the app's functionality and its modus operandi are established, the following improvements could be made:

- Search for ways to improve the indoor positioning of the user. This method should not limit the flexibility of the user to establish as many locations as needed.
- Search for IoT companies that are willing to implement this solution as a second method of authentication for their actions. Work with them to be able to adapt the features to their devices.
- Develop the connection between the system and the service sending the commands to the IoT devices.
- Test it with different IoT devices.
- Create an interface for the companies to manage their devices. With this, companies should be able to add new devices, manage their features, establish the degree of risk of the actions.

Chapter 9. BIBLIOGRAPHY

[1] L. Tung, "IoT devices will outnumber the world's population this year for the first time | ZDNet," *ZDNet*, 2017. [Online]. Available: https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/. [Accessed: 26-Jun-2018].

[2] Steve Ranger, "ZDNet - What is the IoT? Everything you need to know about the Internet of Things right now," *ZDNet*, 2018. [Online]. Available: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/. [Accessed: 30-May-2018].

[3] J. Dyble, "97% of risk pros believe unsecured IoT could facilitate cyber attacks | AI | GigaBit," *Gigabit Magazine*, 2018. [Online]. Available: https://www.gigabitmagazine.com/ai/97-risk-pros-believe-unsecured-iot-could-facilitate-cyber-attacks. [Accessed: 12-Jun-2018].

[4] T. Armerding, "Smart devices get smarter, but still lack security," *CSO*, 2013. [Online]. Available: https://www.csoonline.com/article/2134252/fraud-prevention/smart-devices-get-smarter--but-still-lack-security.html. [Accessed: 26-Jun-2018].

[5] D. Burris, "The Internet of Things Is Far Bigger Than Anyone Realizes | WIRED," *Wired*, 2018. [Online]. Available: https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/. [Accessed: 26-Jun-2018].

[6] M. Elliot, "Two-factor authentication: How and why to use it," *c|net*, 2017. [Online]. Available: https://www.cnet.com/how-to/how-and-why-to-use-two-factor-authentication/.

[7] InfSoft, "Indoor Positioning - Basic Information from infsoft," *InfSoft*. [Online].

Available: https://www.infsoft.com/indoor-positioning. [Accessed: 05-Jun-2018].

[8] D. Palmer, "An Internet of Things 'crime harvest' is coming unless security problems are fixed | ZDNet," *ZDNet*, 2018. [Online]. Available: https://www.zdnet.com/article/an-internet-of-things-crime-harvest-is-coming-unless-security-problems-are-fixed/. [Accessed: 12-Jun-2018].

[9] W. Warne, "Bluetooth Low Energy - It starts with Advertising | Bluetooth Technology Website," *Bluetooth*, 2017. [Online]. Available: http://blog.bluetooth.com/bluetooth-low-energy-it-starts-with-advertising?_ga=2.93385300.835209614.1530008581-186924438.1530008581. [Accessed: 26-Jun-2018].

[10] "What is iBeacon? A Guide to Beacons | iBeacon.com Insider." [Online]. Available: http://www.ibeacon.com/what-is-ibeacon-a-guide-to-beacons/. [Accessed: 26-Jun-2018].

[11] K. Lewis, "Where's my stuff? How location and IoT work well together," *IBM Internet of Things Blog*, 2016. [Online]. Available: https://www.ibm.com/blogs/internet-of-things/location-iot/. [Accessed: 12-Jun-2018].

[12] S. Gokceli, N. Zhmurov, G. K. Kurt, and B. Ors, "IoT in Action: Design and Implementation of a Building Evacuation Service," *J. Comput. Networks Commun.*, vol. 2017, pp. 1–13, Jan. 2017.

[13] "Defense in depth," *OWASP*, 2015. [Online]. Available: https://www.owasp.org/index.php/Defense_in_depth. [Accessed: 02-Jul-2018].

[14] "Double Up on Security With Two-Factor Authentication (2FA)," *Duo Security*, 2018. [Online]. Available: https://duo.com/product/trusted-users/two-factor-authentication. [Accessed: 02-Jul-2018].

[15] M. Rouse, "What is security token (authentication token)?," *TechTarget*, 2005.

[Online]. Available: https://searchsecurity.techtarget.com/definition/security-token. [Accessed: 02-Jul-2018].

[16] R. Brandom, "Two-factor authentication is a mess," *The Verge*, 2017. [Online]. Available: https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess. [Accessed: 05-Jul-2018].

[17] J. Davis, "Two Factor Auth List." .

[18] N. Akhtar and F. ul Haq, "Real Time Online Banking Fraud Detection Using Location Information," Springer, Berlin, Heidelberg, 2011, pp. 770–772.

[19] "Nest Labs," *Wikipedia*, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Nest_Labs.

[20] "Nest | Create a Connected Home," *Nest*. [Online]. Available: https://nest.com/. [Accessed: 02-Jul-2018].

[21] "Wemo | Home Automation," *Belkin*. [Online]. Available: http://www.belkin.com/us/c/home-automation/. [Accessed: 03-Jul-2018].

[22] "Smart Air Conditioner | Control Your AC With Your Phone," *Sensibo*. [Online]. Available: https://sensibo.com/. [Accessed: 03-Jul-2018].

[23] "Meet Hue," *Philips*. [Online]. Available: https://www2.meethue.com/en-us. [Accessed: 03-Jul-2018].

[24] "How Does GPS Work?," *Techwalla*. [Online]. Available: https://www.techwalla.com/articles/how-does-gps-work. [Accessed: 02-Jul-2018].

[25] "How does GPS work?," *physics.org*. [Online]. Available: http://www.physics.org/article-questions.asp?id=55. [Accessed: 02-Jul-2018].

[26] "Mean Squared Error - Definition, Formula & Examples," *TutorVista*. [Online].

Available: https://math.tutorvista.com/statistics/mean-squared-error.html. [Accessed: 10-Jul-2018].

[27] "What Materials Can Block A Wi-Fi Signal? (And What About Interference?)," *Best Wireless Routers Now*. [Online]. Available: http://bestwirelessroutersnow.com/materials-block-wifi/. [Accessed: 05-Jul-2018].

[28] "Which Building Materials Can Block Wi-Fi Signals?," *eyeSaaS*. [Online]. Available: https://eyesaas.com/wifi-signal-loss/. [Accessed: 06-Jul-2018].

[29] "URLSession - Foundation | Apple Developer Documentation," *Apple Developer*. [Online]. Available: https://developer.apple.com/documentation/foundation/urlsession. [Accessed: 04-Jul-2018].

[30] D. Shah, "How to get HTTPS working on your local development environment in 5 minutes," *FreeCodeCamp*, 2018. [Online]. Available: https://medium.freecodecamp.org/how-to-get-https-working-on-your-local-development-environment-in-5-minutes-7af615770eec. [Accessed: 04-Jul-2018].

[31] T. Duong, T. Valverde, and Q. Nguyen, "Bad life advice - Replay attacks against HTTPS | Thiago Valverde," 2016. [Online]. Available: http://blog.valverde.me/2015/12/07/bad-life-advice/#.W0YWGS0rwmJ. [Accessed: 11-Jul-2018].