Instituto Tecnológico
y de Estudios Superiores de Occidente
Reconocimiento de validez oficial de estudios de nivel superior según acuerdo secretarial 15018, publicado en el Diario Oficial de la Federación del 29 de noviembre de 1976.

Departamento de Electrónica, Sistemas e Informática
Especialidad en Sistemas Embebidos

Near Field Communication with Amazon Web Services

TRABAJO RECEPCIONAL que para obtener el **GRADO** de
ESPECIALISTA EN SISTEMAS EMBEBIDOS

Presentan:
MISAEL ÁLVAREZ DOMÍNGUEZ
WILLEVALDO ALEJANDRO FLORES DÍAZ

Asesor **LUIS ENRIQUE GARABITO SIORDIA**

Tlaquepaque, Jalisco. 19 dejulio de 2019.

Acknowledgements

Misael
I would like to express my sincere gratitude to the National Council of Science and Technology for providing the scholarship number 936692 to complete the program, to the ITESO which provides the means to successfully complete the specialization program.

Besides, I would like to specially thank to my family and friends for their support and for the time I could not be with them.

Willevaldo
I would like to express my gratitude to the ITESO University and professors, as well as the National Council of Science and Technology for providing the scholarship number 936692 that gave me the opportunity to do this work, and therefore the specialization program.

Secondly, I would also like to express my special thanks to my family who helped me and encouraged me a lot in finalizing the specialization program.802714

Abstract

Internet of Things (IoT) has become the trending topic of collaborative applications by connecting many kinds of devices together via internet, and thus, allowing flexible solutions for remote control devices. These applications can work together with communication protocols like Near Filed Communication (NFC) to complement secure intended approaches. One concern of embedded IoT devices development is the customized developments which limit portability. The present work aims to show a secure NFC embedded IoT device using the LPC54018_IoT development board working together with AWS, specifically using AWS services Lambda and IoT Core. By working with these elements there is the advantage of using an existing framework for connection, data exchange and cloud code execution. The outcome of the project displays a solution that can authenticate NFC tag devices dynamically using data generated from the cloud service and then, synchronize with the embedded development board. Future improvements can be considered for this project in regards of increased cloud server security and device mobility by migrating to a cellular network based connection.

Keywords— Internet of Things, Amazon Web Services, Near Field Communication, LPC54018

1. Introduction

Internet of Things (IoT) is accelerating the development and innovation offered by the technology sector, such as domestic appliances, medicine, sensor networks, and security solutions. The key characteristics of IoT are the capability to build flexible networks, in other words, with this technology the number of connected devices can increase or decrease according to the needs of the use case, and the ability to control the devices by cloud services. To date the number of devices connected to the internet continues to increase [Reference], as networks become larger and more capable in terms of performance, bandwidth, and speed through protocol and standard innovations, such as 5G, IPV6, and Thread. Furthermore, new compact and energy-efficient devices have been introduced in the market [1]. With the large amount of IoT devices connected to the internet, a secure solution can be flexible by taking the advantage that multiple devices can function as different access points.

Since IoT devices are connected to the Internet, they are susceptible to security breaches. Therefore, a crucial step to accomplish a secure access is the authentication process, which determines the capability for a user, or machine system, to grant or give access to another system. In this way, secure access solutions can be implemented in car rental services, lodging, and parcel pick up points. When the user requests any of these services, access will be granted during the time requested; then, it will be denied once the rental period is over, or when the parcel is retrieved. The request and validation process performed for the secure access service can be handled by an IoT embedded device.

In terms of requesting and validating access, the Robotics Company Nuro, is deploying an autonomous delivery service [2]. The user requests goods via internet, when the autonomous car arrives, then, the user gets a personal identification number (PIN) that will be used to open and retrieve the requested parcel. Instead of relying on a PIN for validation, a secure protocol solution adds security and convenience, like Near Field Communication (NFC). The IoT device acts as a gateway between the NFC device and the cloud, since the user does not need to interact with a human machine interface like PIN validation, and instead only the valid NFC device (eg. smartphone) to complete the operation is required.

1. INTRODUCTION

Regarding authenticating through an IoT device, previous studies show either custom developments, implementing local cloud solutions [3], [4] or not taking advantage of existing IoT development platforms [5], [6]. However, these kinds of projects focus on specific developments leading to limited portability and low reuse. Therefore, the work presented in this paper displays an embedded IoT device integrated with NFC and cloud computing solution for a dynamic access control system (DACS) utilizing an LPC54018_IoT development board, connected with Amazon Web Services (AWS).

2. Methodology

The presented system consists of two main parts: cloud service and embedded IoT device. The cloud service handles two processes: authentication data (Token) generation and distribution to the IoT device, as shown in Figure 2-1. The Token is generated upon request and dictates which NFC tag will be granted access. The embedded device on the other hand, is responsible of stablishing a connection with the cloud service to receive the generated Token. Using this Token, the embedded device is capable of authenticating and grant access to the valid NFC tag.

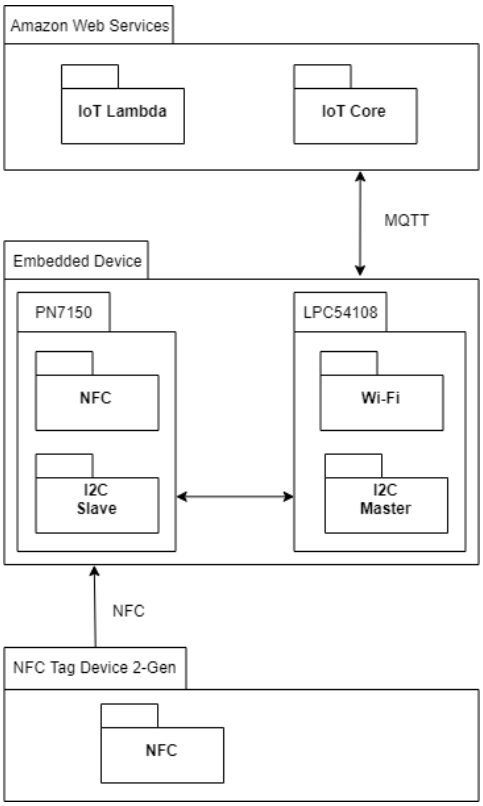

Figure. 2-1 System Architecture

A third component of the system is the tag-type NFC device. The request process will also end up in a tag device storing the Token as well. This implementation is out of the scope for this project, since the only needed input to the system by the Tag, is the token being read by the NFC base station. To display the system, fixed-value-Tokens are stored in different tags, then, the cloud server dictates which tag is valid to be granted access.

2.1. AWS IoT Core

In order to set up an environment on AWS to work in conjunction with an embedded IoT device, a secure framework needs to be created. It consists of creating a policy, certificates, and an embedded device registration. The service in charge of this secure framework is IoT Core. First, the Thing (nomenclature within this service for IoT devices) needs to be registered. After registration, an Amazon Resource Name (ARN) is assigned in order to be identified as a unique resource. Then, security must be linked to the registered device through a certificate and secure policy. The certificate is generated and later used to create header files that will be exported and compiled within the embedded device software. This certificate must be linked to a secure policy that dictates the permissions granted. These privileges defined by the policy allow the IoT device to connect and exchange data with the IoT Core. In order to exchange data IoT Core generates a custom endpoint which routes the information, working together with MQTT protocol.

2.2. AWS Lambda

Once the configuration and setup are ready for cloud and embedded device to work together, the functionalities are programmed at both ends. The service used for the cloud is AWS Lambda, which is a serverless solution meaning that neither managing nor provisioning servers, are required in order to execute code. Within Lambda, applications and functions can be created. For this project, a Lambda function was implemented. Lambda functions can be linked to other AWS services to be treated as triggers or outputs. The trigger to the function can be the request to generate fresh authenticating data. For this implementation that request is generated internally, when the function is triggered the data to be sent is prepared together with the information needed to perform the communication: broker endpoint and MQTT topic. In the other hand, the output of the Lambda function is the message sent to the IoT Core, then data is forwarded to the embedded device via MQTT protocol.

2.3. Embedded IoT Device

The PN7150 NFC module is a plug-and-play NFC solution for an effortless application integration, this module supports the I2C protocol communication which is used to connect with the master device. For the master device implementation, base projects for the K64F microcontroller were reviewed, provided by NXP and based on MCUXpresso IDE. The IDE and SDK can be acceded through the NXP platform [7]. The main functionalities provided by this base project are the connection and configuration of the NFC controller, the handling of the process of NFC discovery, the implementation of the "NDEF protocol", and the HW abstraction to the NFC library. These described NFC components were migrated to a LPC54108 microcontroller.

The LPC54108_IoT development board was designed for developments with connections to AWS. Therefore, it makes it suitable for this project development. The resources provided by the manufacturer include libraries and drivers to control the peripherals and hardware included in the development board, like the Wi-Fi module, used to stablish the internet connection. After connecting to internet, the cloud service requires two resources in order to allow connection and route communication: security certificate and broker endpoint. The certificate is handled as a header file in the software, while the endpoint is a constant in the code used only when attempting to connect to AWS. Then, this link is preserved to sync authenticating data between AWS and the LPC54018_IoT.

3. Results

As expected, the PN7150 NFC module was able to detect and read information from tag devices within 5cm and with a latency of 366 milliseconds. Thus, I2C transfers data at 100 kbps. While the low latency is covered from the embedded NFC side, a stable connection between AWS and the embedded device, must also be assured. To verify the connection reliability an instrumented code was implemented, it works as follows: upon connection, the embedded device publishes a message to AWS, then a disconnection is requested, when the disconnection is confirmed, a new connection request is triggered. This loop was repeated for four hours. Figure 3-1 captured from IoT Core monitoring tool, shows the successful connections during the testing time. Maximum 15, minimum 12, recorded with a sample rate of 5 minutes.

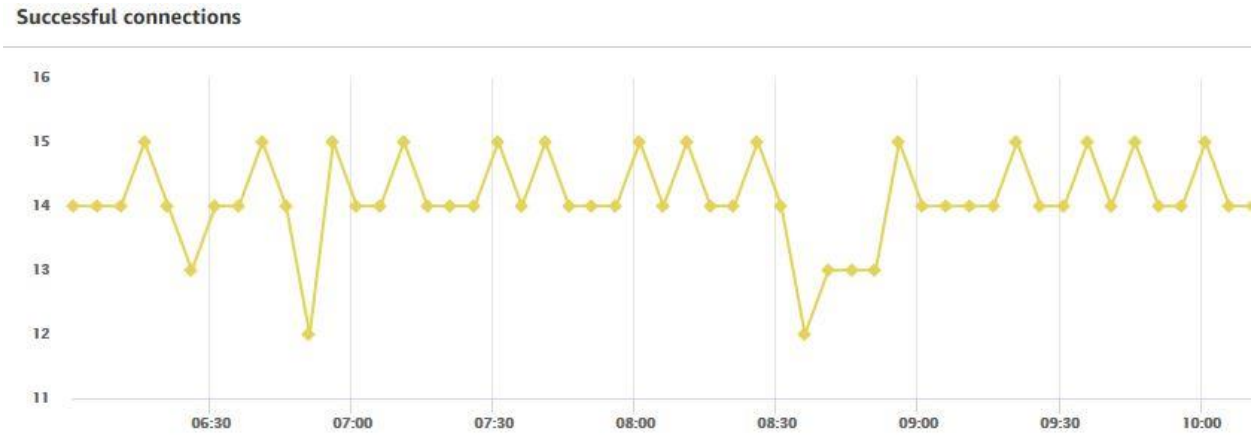

Figure 3-1 Successful connections record from IoT Core

4. Conclusions

The outcome of the presented work shows the advantage of implementing an IoT embedded device in conjunction with the existing AWS platform. This approach allows to focus on application development since the supporting topics for the development like communication and server provisioning are already provided by the platform. For the application, both AWS and the embedded device seamlessly work together to control authentication data and validate NFC tag devices. The success of this project relies on performing the operations with low latency, reliability, and security.

Regarding future work, four topics were identified as potential updates for the system: analyze cyber security use cases, upgrade the internet link to a cellular network based device, counterpart complementary project (Smartphone for triggering and authenticating), and upgrade NFC tag devices to newer generation and authenticate directly from cloud.

References

[1] V. D. Vaidya and P. Vishwakarma, "A Comparative Analysis on Smart Home System to Control, Monitor and Secure Home, based on technologies like GSM, IOT, Bluetooth and PIC Microcontroller with ZigBee Modulation," in 2018 International Conference on Smart City and Emerging Technology (ICSCET), 2018, pp. 1–4.

[2] "Delivering Safety Nuro's Approach" [Online]. Available: https://nuro.ai/. [Accessed: 19-Jul-2019].

[3] M. H. Alharbi and O. H. Alhazmi, "Prototype: User Authentication Scheme for IoT Using NFC," in 2019 International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1–5.

[4] Y. Choi, Y. Choi, D. Kim, and J. Park, "Scheme to guarantee IP continuity for NFC-based IoT networking," in 2017 19th International Conference on Advanced Communication Technology (ICACT), 2017, pp. 695–698.

[5] N. Nikolov, "Research of the Communication Protocols between the IoT Embedded System and the Cloud Structure," in 2018 IEEE XXVII International Scientific Conference Electronics - ET, 2018, pp. 1–4.

[6] H. Hejazi, H. Rajab, T. Cinkler, and L. Lengyel, "Survey of platforms for massive IoT," in 2018 IEEE International Conference on Future IoT Technologies (Future IoT), 2018, pp. 1–8.

[7] "MCUXpresso SDK Builder." [Online]. Available: https://mcuxpresso.nxp.com/en/welcome. [Accessed: 19-Jul-2019].