Analysis of Security Functions of a Cryptochip in a IoT Device with Amazon Alexa and AWS Services

Juan Carlos Araiza Jimenez[1], Dreysy Pozos González[2], Elizabeth Pérez Aguilar[3], José Crispín Hernández Hernández[4], Edmundo Bonilla Huerta[5]

[1, 2, 3, 4, 5]Tecnológico Nacional de México/ Instituto Tecnológico de Apizaco, Apizaco, Tlaxcala, México

m19371363[at]apizaco.tecnm.mx, m19371373[at]apizaco.tecnm.mx, m19371374[at]apizaco.tecnm.mx, crispin.hh[at]apizaco.tecnm.mx, Edmundo.bh[at]apizaco.tecnm.mx

Abstract: ***In the recent age of modernization, the concept of IoT is like a game changer as it enables us to move towards smart world by the concept of connecting multiple things through the use of internet. IoT Enablers are used for this purpose. These enablers aid the connection of IoT to that of electronic equipments. Cryptochip Technology is like a smart card that is based on encryption technology. The linkage of IoT with Cryptochip Technology is what we done in this study. There were many case studies done for this purpose but the research in this field is ever - growing. Micro - Control - Units are what we used for this purpose. They contain a WIFI module and a Cryptochip in order to chip data from AWS Cloud. In next step, AWS Cloud connection and Programming was done. In later step, there's need to upload those programs to library. SO, USB is used for this purpose. Those programs are then configurated and is made ready for use. This can strengthen the concept of smart store and could be used as another step forward in terms of cloud technology.***

Keywords: MCU, Cryptochip, Authentication

1. Introduction

Internet of Things (IoT) is the systematic administration of objects containing electrical equipments embedded inside their structurein order to convey and to detect for the purpose of linking either with each other or with the climate (external). Internet of Things (IoT) alludes to a wide vision in which „things" like the regular objects, spots and conditions which can be interconnected with each other through the Internet. A straightforward illustration of an IoT object which is presently accessible in a portion of the homes is an indoor regulator which can be utilized to decide regarding when an individual consume certain rooms and modify the degrees of warming, lighting and different capacities in the house likewise. By expanding the Internet from "a network of interconnected PCs to a network of interconnected objects. " the Internet of Things (IoT) will incorporate an assorted what's more, tremendous network of interconnected gadgets. By the use of IoT, it's made possible to link many devices of daily life with smart technology. The main components of IoT are Embedded system (Low Power), Cloud Computing, Data Availability and Network Connection (Carretero 2013) . All these components work together is order to enable the linkage between the devices normally known as smart technology. This all can be achieved in 2 ways: Using of Separate Network that contains physical objects, use of hardcore technology in order to enable cloud technology for the purpose of data storage. The later requires modern technology and is expensive because it requires large memory in order store data. For the purpose of enabling the IoT, there are certain enablers used. Some are RFIDs, Sensors and Smart Technology. These enablers help the systems to connect with each other by means of physical signals in order to be able to develop wat we know as IoT. The main characteristics of IoT are what make it among the most anticipated technology in this modern era. Some of these are: Efficient and Scalable, Less Power Consumption, Getting a rid of IP based connectivity etc. These characteristics symbolize the importance of IoT and the reason why it means to conquer every other technology of this modern world. The areas of applications of IoT are manufacturing business, security, healthcare business etc. Apart from these, it's finding its feet strong in the areas of smart grid technology, smart homes, smart cities, Detection of Earthquakes etc. These all areas also highlight the importance of IoT (Botterman 2009) .

IoT technology is also being used in the areas of Cryptochip technology. This technology is like a smart card which is used by the help of an encryption controller in order to avail associated services. It's like a smart Credit card. In this area, usage of IoT can aids in liking the devices of common use to that to Cryptochip in order to avail the services quickly without thinking about the security hazards as the encryption of Cryptochip is among the safest encryptions. Thus, IoT can help us in linking the devices of modern use like that of Alexa of Amazon and AWS Cloud based technology. By enabling this, these services can be used at finger tips. Moreover, the upcoming era is bound to be of chips because of their fast working and smaller size. So, enabling IoT also aids modernization (Brush 2011) .

In this article, we'll discuss how we can enable the linkage of IoT in Cryptochip by the use of Amazon's Alexa and AWS Cloud Services. We'll discuss the research methodology adopted, the results obtained and also the potential hindrances that this technology can face when launched. All this will be discussed along with the conclusion that we will draw by observing the research methodology.

2. Study of Related Work

Before moving onto the research methodology, there's need to study and understand the previous work done in this case in order to be able to develop and linearize the area of research we need to done with proper understanding of what needs to be done in order to improve what has done in previous studies. When we study the work that will be introduced beneath, we can say that the programming and the evolution of the devices are quite updated and is continually refreshed, this has permitted the creation and development of IoT devices, yet as per these studies, we should refresh ourselves in information on the best way to work it. This all will be done without failing to remember the significance of its security. The term TLS has effectively existed for quite a long time, this is the principal layer of safety that TLS utilizes certificates to connect keys and names. A certificate joins a distributed key with other data, for example, the name of the help that utilizes the key, and this blend is carefully endorsed by another key.

Since this venture is associated with the cloud technology, it’ll works through Amazon Web Services, however the normal layer is TLS, yet similarly, this layer includes a capacity inside Secure Sockets to make coordinated applications to impart safety. The library is intended to make it simple for programming engineers from different network programming foundations to join their work. This FreeRTOS Secure Sockets library depends on a TCP/IP stack and a TLS execution (Red) .

We can discuss a TLS customer starting an association by trading messages with a TLS worker. For some application protocols, look into the worker’s name utilizing DNS to get an Internet Protocol (IP) address. For this situation, AWS can do it, dependent on keys created by IAM, Amazon's administration itself, for which they are extraordinary, modified in the Amazon CLI along with the Endpoint that decides the locale of the worker to be created.

Concerning referencing in the task, they allude to the way that nodes that have the secret key can recuperate the first worth, through a straightforward hunt inside the designation table created already. The HMAC mapping technique is ideal for conditions where the data delivered is restricted or inside certain worth reaches (e. g., temperature sensor). On account of AWS, we can discuss the way that an assistance that it has is in IoT Core. Concerning the work to be referenced, we will zero in on security and data assurance since it is an extremely referenced and reprimanded point inside the development of IoT devices, we will show the security and creation of every framework inside equipment and programming in the cloud (S. Huh 2017) .

3. Research Methodology

With the fast - paced modernization of present era, it is in our utmost favor in order to save time by connecting the devices of daily use to internet due to which it will be easy to control them. Doing so will save our time as time is the real money now - a - days. This is made possible by the evolution made through IoT. Using IoT, we can achieve this goal by connecting our devices to either WIFI or to MCU. Example of this technology can be observed in shape of WIFI controlled air conditioners etc. As in this research, we need to work on the encryption of IoT with Cryptochip, so, we’ll talk about MCU in this report.

The research methodology along with the required materials is as follow:

3.1 Study of Microcontroller unit

The MCU contains a WIFI module for the web association and a Cryptochip to ensure the data that is shipped off the AWS cloud to keep our information as secure as could really be expected. MCU (Micro - Controller Unit) has a place with the class of advanced hardware and is an assortment of huge scope circuits. This little coordinated circuit is responsible for controlling the various functions of a gadget, be it's anything but, a TV control or a computer game control center controller. The MCU, shown I figure, is constrained by the WINC1510 module like the one displayed in figure 1. This permits us to make an association with a Wi - Fi network to design the card with the AWS administrations. The boundaries that permit us to acquire this card are those of Temperature, pressure, humidity. What's more, it permits us to control 2 Light Emitting Diodes (LEDs), which can be utilized in an many different ways, contingent upon what you need to utilize the card for.

Figure 1: WINC 1510 MCU

3.2 AWS Cloud connection

The MCU runs AWS IoT SDK pre - stacked, libraries utilized by IoT gadgets to assist them with interfacing the AWS IoT cloud, this SDK incorporates a cloud association API alongside the Machine to Machine (M2M) correspondence convention for correspondence between IoT gadgets MQTT, (Message Quiring Telemetry Transport), is gotten from the HTTP association convention as the reason for correspondence. The distinction between these 2 is that the HTTP convention conveys through the solicitation reaction model, while the MQTT convention imparts through the distribute buy in model it is an exceptionally summed up execution of the Internet of Things, it contains sensors, control boards or portable applications. The procured information goes through numerous switches and switches. In the MQTT convention, three principal elements partake.

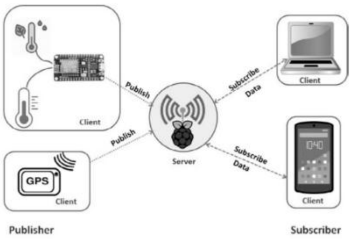


Figure 2: MQTT Configuration

1) **Publisher** gathers information from gadgets, for example, the sensors that they have executed, for example, the temperature of the temperature sensor that

we have in the washroom of our home. The point would be "/home/room/temp - sensor"

2) **Subscriber** buys in to the theme that Publisher is distributing "/home/room/temp - sensor", the subscriber can be both a cell phone and a control board.
3) **Broker** gathers the information from Publisher and supplies it to Subscriber.

The MQTT client ID is needed for the association and the client key identifier (Subject Key Identifier SKI) of the gadget that is utilized as the MQTT client ID. This ID can be acquired by examining the QR code of the card and the client secret key can be given through the AWS Cognito administration.

The board makes the association with the AWS IoT cloud with the TLS encryption suite. The gadget testament and the private key are put away in the ECC608 crypto - validation gadget that contains the board, as can be found in figure 3. The MCU utilizes the endorsement and the key in the ECC608 to confirm with the cloud. AWS IoT. In this manner our accreditations and individual information are safer and secured, they are essentially difficult to capture by outsiders with noxious goals.

3.3 Programming

The programming of the board is through a USB link, in this way we can stack our own projects: The SAM - BA V2.18 programming is utilized to stack the design program to the board. To program the card, the primary thing to do is interface the USB link to the charging port of the board prior to associating it to the USB port of the PC or PC, when the USB link is associated with the board you need to keep squeezed the fundamental fasten and associate the USB link to the port of the PC, this is done in a way that the board enters troubleshooting mode and, in this manner, to have the option to stack the programming documents. To know whether the board has entered troubleshooting mode, the pc or PC that we are utilizing should make a sound to affirm the association of an outside gadget, for example, when we interface a USB or an outer hard drive and the board ought not have no driven on.

3.4 Configuration

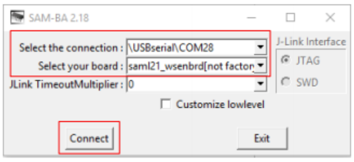
As USB or Card is required to upload the Configuration files to the library, we've the following two files for configuration process.

- saml21g18b_sensor_board_demo_JITR. atsln
- saml21g18b_sensor_board_demo_ECC. atsln

The 2nd file is used for the establishment of AWS account. By opening it, an authentication key will be generated, that's used to configure the IoT with AWS. These keys are safely encrypted in Cryptochip.1st File is used for the subscription of AWS with IoT.

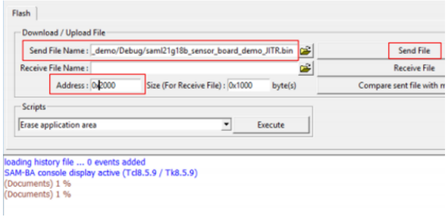
3.5 Uploading Files to the Library

First of all, you need to place the board in investigate mode to have the option to stack the 2 documents vital for the design of the board. When the card is in investigating mode, we will open the Sam - Ba programming, the variant being referred to is 2.18, when the samba is open, it should be arranged in "Select the association" \USBserial \COM28 is set to tell the program that the arrangement will be completed by USB, in "Select your load up" our card is chosen for this situation it would be saml21_wsenbrd, in "JLink TimeouMultipler" it is left at 0, trailed by unchecking "Alter lowlevel" and click on Connect. Tapping on Connect will show us another window, here the records are stacked, for this you need to go to the "Streak" segment. In the place of "Send File Name" the main record saml21g18b_sensor_board_demo_ECC. atsln is chosen, in "Address" we will choose the memory address 0x2000 and click on Send to stack the document to the board.



Select the connection : \USBserial\COM28
Select your board : saml21_wsenbrd[not factory
JLink TimeoutMultiplier : 0
☐ Customize lowlevel

Figure 4: Main Window's Configuration



Send File Name : _demo/Debug/saml21g18b_sensor_board_demo_JITR.bin
Receive File Name :
Address : 0x2000 Size (For Receive File) : 0x1000 byte(s)
Erase application area

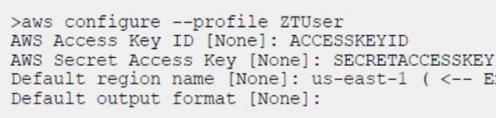
```
loading history file ... 0 events added
SAM-BA console display active (Tcl8.5.9 / Tk8.5.9)
(Documents) 1 %
(Documents) 1 %
```

Figure 5: Procedure for Uploading File

Configurating saml21g18b_sensor_board_demo_ECC. atsln

Prior to designing our saml21g18b_sensor_board_demo_ECC. atsln document, it is important to make an I Am client and arrange the AWS CLI:

- We make the I AM client by entering the AWS I Am administration with our AWS account, here our client is made, we simply give it an exceptional name and fill in the fields that we are requested and when our I Am client is made, we are will allow a CSV document that contains an ACCESSKEYID and a SECRETACCESSKEY which we will use for the setup of our board.



```
>aws configure --profile ZTUser
AWS Access Key ID [None]: ACCESSKEYID
AWS Secret Access Key [None]: SECRETACCESSKEY
Default region name [None]: us-east-1 ( <-- E
Default output format [None]:
```

Figure 6: Access/Secret Access Key

- To design the CLI (Command Line Interface) it is important to have the AWS and Python CLI apparatus, with these 2 devices we open a terminal and execute the accompanying order AWS arrange - profile "user_name_I_Am", when executing this order, the section of an ACCESSKEYID, a SECRETACCESSKEY and the name of an area will be mentioned as displayed. we duplicate the entrance keys from our CSV and the name of the district is given as us - east - 1. Having the CLI designed, we continue with the arrangement of the saml21g18b_sensor_board_demo_ECC. atsln document, we should go to the area of the record in the terminal that we are utilizing Python _CreateCertsAndRegister2AWS.

py - profile <name of your - AWS - cli - profile>. This order access endorsements alongside their private keys.

- We continue to arrange our card to a Wi - Fi network with the order Python _CreateCertsAndRegister2AWS. py - profile <name of your - AWS - cli - profile>, we should enter the SSID and secret key of our Wi - Fi organization. The order plays out the accompanying assignments:
- Save the Wi - Fi association SSID and secret word in ECC608
- Requests the Cryptochip ECC608 to create a mark testament, which stays private when put away in the crypto
- Receives the declaration marking demand (CSR) and signs it with the private key
- Returns it for capacity to the ECC608

Configuring saml21g18b_sensor_board_demo_ECC. atsln:

We rehash the above interaction, open Sam - Ba and burden the saml21g18b_sensor_board_demo_JITR. atsln record with a similar memory address 0x2000. The primary drove will start to streak blue at a normal speed, this implies that the card is attempting to associate with the district that we showed during the CLI arrangement, later the drove will start to streak quicker similarly in blue, this demonstrates that the board has effectively settled an association and gotten the IP address. At last, it turns strong blue, demonstrating that the board has effectively associated with the AWS cloud.

4. Conclusion

With the Internet of things, it is workable for us to have our gadgets that we use consistently associated with the organization, yet it is simpler with the administrations that Amazon accommodates this, however commonly the gadgets don't have great security and are helpless against assaults, being along these lines, regardless of how immaterial it might appear in the event that we have associated our lights to the organization, yet the gadget we use doesn't have a Cryptochip and by chance our security is compromised, the aggressor can liquefy our lights and cause a short in our electrical organization and render it futile. However, with a Cryptochip that stores our qualifications and access keys, this turns out to be more muddled and we are better secured against assaults. The major work in this case was done in previous studies. By the use of that work through upgradation, we configurated the Amazon’s Alexa to IoT using MCU. This can lead to strengthen the concept of smart store and could be used as another step forward in terms of cloud technology.

References

[1] Botterman, M. (2009). " Internet of Things: an early reality of the Future Internet. " Report of the Internet of Things workshop. European Commission Information Society and Media Directorate General at Prague.
[2] Brush, A. J. B., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S. & Dixon, C. (2011). "Home automation in the wild: challenges and opportunities" ACM Press.
[3] Carretero, J. G., J. D. (2013). "The Internet of Things: connecting the world. " Personal Ubiquitous Computing.
[4] Red, V. A. ""Practical comparison of distributed ledger technologies for IoT"
[5] " Proc. SPIE 10206, Disruptive Technologies in Sensors and Sensor Systems.
[6] S. Huh, S. C. a. S. K. (2017). "Managing IoT devices using blockchain platform" 19th International Conference on Advanced Communication Technology (ICACT).