Journal of Advanced Research in Technology and Management Sciences (JARTMS)
Volume: 02 Issue: 04 ISSN: 2582-3078 July 2020
Available online at: http:// www.jartms.org

LOW COST AND LOW POWER INNOVATIVE SECURITY ARCHITECTURE FOR IOT DEVICES

[1] KANDULA DHANA LAKSHMI, [2] RAJU THOMMANDRU.
[1]M.Tech Scholar, Dept. of ECE, Chalapathi Institute of Technology, Guntur district, A.P.
[2]Assistant Professor, Dept. of ECE, Chalapathi Institute of Technology, Guntur district, A.P.

ABSTRACT: This paper presents an Arduino board which gives minimum power consumption at a reasonable cost. The security of this technique will be handled by a secure element. By using general purpose unit (GPU) the maximum internet of things (IoT) devices will be developed. The GPU is associated to a radio System on Chip (SoC). In this paper advanced four quarter security architecture will be developed for IoT design. A secure element will be functioned as identity module that executes transport layer security (TLS) packets, and sensor/actuator devices. The TLS secure element worked as an applicative firewall. The Aurdino based microcontroller is used to get low power consumption with low cost. This paper performs experimental platform, realizing a connected thermometer object, built around an Arduino microcontroller, cheap Wi-Fi SoC, commercial java card and temperature sensor.

KEYWORDS: Internet of Things; Security; Secure Element, TLS, SoC, and GPU.

* Correspondence Author

[1] ***KANDULA DHANA LAKSHMI,***

[2] ***RAJU THOMMANDRU.***

[1]M.Tech Scholar, Dept. of ECE, Chalapathi Institute of Technology, Guntur district, A.P.

[2]Assistant Professor, Dept. of ECE, Chalapathi Institute of Technology, Guntur district, A.P.

LOW COST AND LOW POWER INNOVATIVE SECURITY ARCHITECTURE FOR IOT DEVICES

I. INTRODUCTION

This in today's world risk of intrusion has increased in the developing technology. Crime prevention using remote monitoring is one of the aims of current Study. There are several monitoring systems such as camera, CCTV etc. However, today even if the person is moving from one place to another place person can monitor and prevent the criminal activity. A video surveillance system is important in different Fields of our environment such as in personal security, banking, etc. However, it is expensive for normal peoples to set up such Kind of system so the peoples are using IOT based low cost security systems which will help them for secure their commercial places. In raspberry Pi based home security systems sensors are installed to detect the intruders, and alarm is generated. Raspberry Pi security system uses wireless technology and smart phones for security purpose. The main Benefits of the current security systems is simple to implement, Small size portable capable with immediate alert, truly Low-cost for residential use. The Raspberry Pi based security system focused to save valuable lives, money and time. A network of connected things is known as Internet of Things.

Now a day's security is measure requirement in society. As described by a manufacturer, an attack on smart bulbs will be major concern of connected home lighting. This attack executes remote reconstructing from automatons or vehicles, and empowers the infusion of infection. These bulbs are worked over ATmega2564RFR2 SoCs, containing 8-bit microcontroller, 256KB of FLASH, 32KB of SRAM, AES hardware accelerator, and IEEE 802.15.4 radio transceiver. It relies upon two threats: initial a bug on Zigbee stack which is reset to factory and then joins a malicious system; second the embedded AES key is identified thanks to a Correlation Power Analysis (CPA) attack. Since these devices share a similar key, malicious software updates can be performed. In this paper, present secure low cost object, mechanized by an Arduino board and interfacing with a mobile application. The security for the most part relies upon a secure element, with a smartcard form factor. It is applied by a one of a kind TCP server with assistance of notable 443 (TLS) port. The TLS stack runs in the secure element (SE) and executes a solid shared validation dependent on X509 authentications between two gatherings. So the SE works like an alter safe firewall that verifies approaching associations. More generally the demonstrated object realizes a four quarters secure architecture, worked more than four components. A General Purpose Unit (GPU) facilitates three devices

1) A SoC responsible for charge of communications
2)A secure element performing TLS convention tasks and characterizing object identity
3) Sensors and actuators constrained by the GPU.

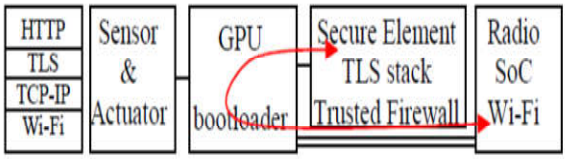

Fig. 1: Four Quaters Security Architecture, Based On Secure Element.

Network of several connected things is known as Internet of Things (IoT). Here the objects are based on computers controlling sensors and/or actuators, including radio resources and communication stacks. Based on their computing capabilities, generally there are three classes of IoT nodes, according the RFC 7228. They are

1. The C0 devices (RAM size << 10KB, code size << 00KB)
2. The C1 devices (RAM size #10KB, code size #100KB)
3. The C2 devices, (RAM size #50KB, code size #500KB)

II. LITERATURE SURVEY

The entry of the exponential advancement of the internet-of-things (IoT) due to the quick development of internet-connected smart objects. As the number of connected smart-objects increase, IoT will continue to advance by providing connectivity and interactions between the physical and the cyber world. This connectivity is characterized by low throughput, delay sensitivity, small and wide coverage, low power consumption, low device, etc. that explains the emergence of low power wide area network (LPWAN). LPWAN technologies are alternative promising connectivity solutions for Internet of Things. However, the lack of an overall LPWAN knowledge that present a comprehensive analysis of LPWAN technologies is presently constraining the achievement of the modern IoT vision. In this paper, we begin with a detailed analysis of the conventional high power long-range network technologies that considers IoT applications and requirements. Cloud security is one of the active research areas and extensive research work has been carried out in recent years. A number of effective techniques have been proposed by various authors to provide security to cloud data and information. This chapter discusses several works done by various researchers that deal with cloud data centric security.

Data security and access control is one of the most challenging ongoing research work in cloud computing, because of users outsourcing their sensitive data to cloud providers. Before choosing different types of encryption techniques, it is important to choose methods for generating keys. Several authors have discussed various types of key generation techniques and key management. We have found different papers related to security system. Different security systems used for different purposes. Sushma.N. Nichal, Prof. J.K. Singhhas done abstraction of Smart supervisor system using IOT based on embedded Linux O.S. with ARM11 architecture. In this Paper they have implemented real-time video monitoring system and acquired data. In this system they have also used PIR, temperature, Humidity sensors the system first requires authentication from user to activate the system if the system detect human it will send that data to the server or user smart phone. Sowmiya. U, Shafiq Mansoor. J. Have developed to connect any door with internet, in this system user also implemented PIR sensor and camera. PIR sensor used for detecting person and camera used for capturing the video of person comes at door. The video will be send through 3g dongle to authorized person. They have also discussed some advantages of this system. They have concluded use of this system like bank, hospital etc.

In this paper we present an innovative four quarter secure architecture for class C1 device. Our experimental board comprises four components.
1) An Arduino microcontroller, without operating system, manages the system, and realizes a connected thermometer service.
2) A secure element providing tamper resistant computing resources, in particular a TLS stack.
3) A Wi-Fi interface is provided by a dedicated SoC chip.
4) A temperature Sensor. Thanks to these features this system realizes a connected secure low cost, low power thermometer.

LOW COST AND LOW POWER INNOVATIVE SECURITY ARCHITECTURE FOR IOT DEVICES

III. A FOUR QUARTERS SECURITY ARCHITECTURE

All the IoT electronic boards incorporate a GPU (General Purpose Processor) and related memory like FLASH and RAM. The system is constrained by a operating system, or is instated from a boot loader. Cryptographic methods might be utilized for secure updates or secure boot, when code is sent from non volatile memory to internal or external RAM. A committed chip is required for giving radio assets. Radio protocols are typically secure by a symmetric cryptographic algorithm and its related key. The system On Chip (SoC), for instance conveyed in associated bulbs, coordinate a GPU, radio transceivers, memories and crypto processor. Sensors and actuators are overseen by GPUs, trading messages with the system.

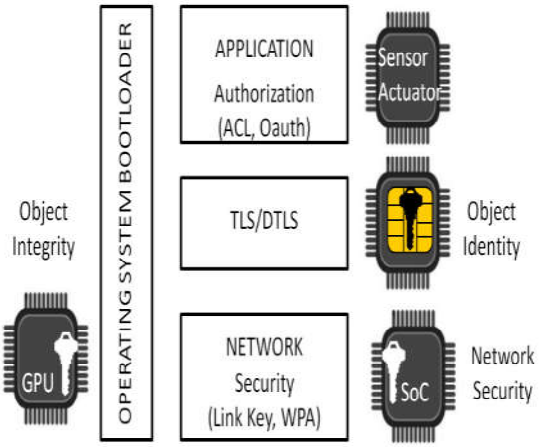

Fig.2. Four Quarter Architecture

The figure 2 represents our idea of four quarter architecture, which includes four substances:

1) A General Purpose Unit that deals with the article. A secure boot needs the validation of the code downloaded in the GPU memory. A safe update follows the same prerequisite. As examined previously tamper resistance computing and key enhancement are expected to maintain a strategic distance from side channel assaults and malicious updates.
2) A radio SoC. This device installs a microcontroller that deals with the communication protocols and edge trades. A symmetric cryptographic key upholds packet integrity and protection.
3) An object identity module. The TLS/DTLS stacks running in secure elements. Since numerous IoT systems use TLS/DTLS for node confirmation, such secure element go about as character modules. In our setting both customer and server are outfitted with X509 certificates and asymmetric keys, they implement solid mutual authentication needed for the arrangement of TLS/DTLS meetings.
4) Sensors and actuators are constrained by the GPU. Approaching DTLS/TLS messages got from the radio interface, are unscrambled, checked, and parsed by the GPU, which controls actuators and sensors. From that point the gathered data is safely transfer to the DTLS/TLS session. Communications are taken care of by the radio SoC. All messages sent/got to/from the GPU are embodied in TLS record layer packet. In this manner the personality module goes about a useful firewall between the item and the system.

Journal of Advanced Research in Technology and Management Sciences (JARTMS)
Volume: 02 Issue: 04 ISSN: 2582-3078 July 2020
Available online at: http:// www.jartms.org

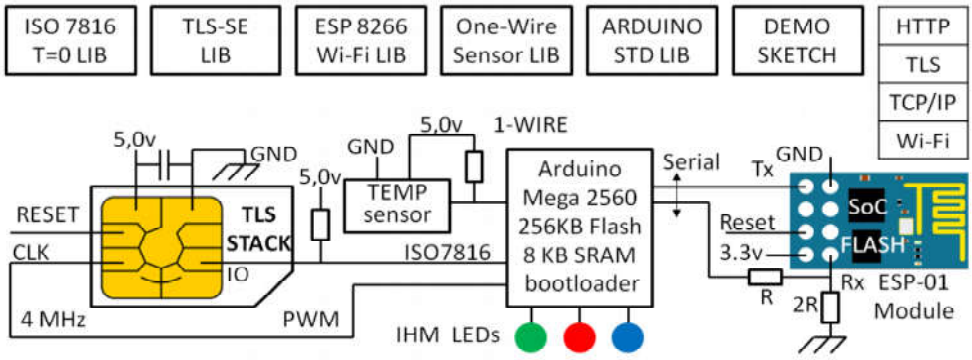

Fig. 3: Connected Thermometer Using Four Quater Architecture

A. The GPU: Arduino Mega

The GPU is an Arduino Mega board, based on ATmega2560 8-bit micro-controller, clocked at 16 MHz, and consists 256 KB of FLASH, 4 KB of EEPROM, and 8 KB of SRAM. The processor has no operating system, and is originated from a 8KB boot loader; it controls various digital input/output pins, and provides PWM (Pulse Width Modulation) facilities. Communications with Wi-Fi SoC, secure element, and temperature sensor are based on serial links. The limited SRAM size is the most critical resource.

B. Identity Module and TLS stack

Secure Element Secure elements are defined by ISO 7816 standards and are usually supporting Java Virtual machine, running software written in the javacard language. From a hardware point of view an ISO7816 device has 5 pins: Vcc, ground, clock, IO and reset. The chip is directly powered by an Arduino digital output, and is activated on demand. The clock is generated thanks to a PWM facility at the 4 MHz frequency, leading, according to the ISO7816, to a basic bit time of 372/4 MHz (about 93µs). Nerveless this time (named ETU) is divided by two in the working mode (372 /2/ 4MHz) thanks to an ISO7816 procedure called PTS (Protocol Type Selection). A byte needs 12 bits (1 start, 8 data, 1 parity, 2 stops), so the useful throughput is about 1792 bytes/s. The ISO7816 driver manages the single serial IO pin and uses a timer resource (a 16 bit counter with a resolution of 1/16 µs) to sample incoming bit stream and to generate outgoing binary signal. It implements the T=0 protocol widely used by SIM cards.

C. Communication Module (Wi-Fi SoC)

The Wi-Fi SoC (ESP 8266) have two parts, an analog area dealing with radio resources, and a processor with at the most 36KB of SRAM associated to an external SPI FLASH, up to 4 MB. The chip implements the IEEE 802.11i security protocol and provides a TCP/IP stack with client and server features. It is managed thanks to well known AT commands, from a serial interface of which we fix the baud rate to 38400 bauds. On the Arduino side the reception and transmission buffer sizes are respectively set to 256 and 128 bytes. The reception (Rx) link is monitored by a

dedicated (and unique) procedure, all incoming events such as TCP session opening and closing, data reception, data transmission confirmation, and errors, are notified by dedicated messages.

D. Sensors & Actuators

Our device is equipped with DS18B20 digital temperature sensor, manufactured by the Dallas Semiconductor company. The sensor works over a proprietary 1-Wire® protocol, which enables the use of multiple devices.

IV. CONCLUSSION

This paper was presented an Arduino board which gives minimum power consumption at a reasonable cost. The security of this technique has handled by a secure element. By using general purpose unit (GPU) the maximum internet of things (IoT) devices was developed. The GPU is associated to a radio System on Chip (SoC). In this paper advanced four quarter security architecture was developed for IoT design. A secure element can functioned as identity module that executes transport layer security (TLS) packets, and sensor/actuator devices. The TLS secure element worked as an applicative firewall. The Aurdino based microcontroller is used to get low power consumption with low cost.

V. REFERENCES

[1] P.Urien, "An Innovative Security Architecture for Low Cost Low Power IoT Devices Based on Secure Elements", demonstration at the IEEE CCNC 2018 conference and at the CES 2018 ComSoc Kiosk.

[2] P. Urien, "Introducing TLS/DTLS Secure Access Modules for IoT frameworks: Concepts and experiments", IEEE ISCC 2017.

[3] E. Ronen, C. O'Flynn, A. Shamir, A. Weingarten, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction", 2017 IEEE Symposium on Security and Privacy.

[4] IETF draft, "TLS and DTLS Security Modules", draft-urien-uta-tls-dtlssecurity- module-04.txt, June 2017.

[5] P. Urien, "Securing The IoT With TLS/DTLS Server Stacks Embedded In Secure Elements: An ePlug Usecase", IEEE CCNC 2017.

[6] Colin O'Flynnn, "A lightbulb Worm?. Details of the Philips Hue Smart Lighting Design", Black Hat USA 2016 .

[7] Ms. RenukaChuimurkar, Prof. Vijay Bagdi, "Smart Surveillance Security &Monitoring System Using Raspberry PI and PIR Sensor", International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-1, January 2016 ISSN: 2395-3470 .

[8] C. O'Flynn, "A Lightbulb Worm? Details of the Philips Hue Smart Lighting Design", White Paper, Black Hat USA 2016.

[9] ShivprasadTavagad, ShivaniBhosale, Ajit Prakash Singh, Deepak Kumar, " Survey Paper on Smart Surveillance System", International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 02 | Feb-2016 e-ISSN: 2395 -0056, p-ISSN: 2395-0072 White Paper.

[10] Khushbu H Mehta, Niti P Gupta, "Vision Based – Real Time Monitoring Security System for Smart Home", Vision Based – Real Time Monitoring Security System for Smart Home, Vol. 4, Issue 2, February 2016 ISSN(Online): 2320-9801 ISSN (Print): 2320-9798.

[11] Eyal Ronen, Adi Shamir, "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights (Invited Paper)", 2016 IEEE European Symposium on Security and Privacy.

[12] Sushma.N.Nichal, Prof.J.K.Singh, "Raspberry pi Based Smart Supervisor using Internet of Things (IoT)",International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 4, Issue 7, July 2015, ISSN: 2278 – 909X.

[13] Sowmiya .U, ShafiqMansoor.J., "Raspberry Pi based home door security through 3g dongle", International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015,ISSN 2091-2730 .

[14] "Rebooting the IT Revolution: A Call to Action" (SIA/SRC), 2015 .

[15] RFC 7228, "Terminology for Constrained-Node Networks", IETF May 2014.

[16] Atmel AVR ATmega2564RFR2 Datasheet, "8-bit Microcontroller with Low Power 2.4GHz Transceiver for ZigBee and IEEE 802.15.4", 2014.

[17] Pretz, K. (2013). The Next Evolution of the Internet.[cited 2013 May 20]; available from http://theinstitute.ieee.org/technology-focus/ technology-topic/the-next-evolution-of-the-internet.