Implementation of Common Secure Framework for IoT based Arduino Platform

Asst. Prof. Dr. Mazin S. Al-Hakeem [#1] , Prof. Dr. Ala'a H. Al-Hamami [*2]

[#] *Department of IT, Lebanese French University (LFU), Kurdistan Region, Iraq*

[*] *Faculty of Computer Science and Informatics, Amman Arab University, Jordan*

Abstract *In the recent years, everything like refrigerators, cars, fans, lights, sprinklers are interconnected to create a better world for human beings, these devices are now collectively called the Internet of Things (IoT). While IoT have made life easier, they have also created new attack area for hackers especially internal attack issues. The number of connected IoT devices constantly increases and becomes more pervasive in our lives, this implies that the security concerns must also constantly increase, especially when considering multiple IoT devices in an interconnected home or business. There is a need for devices trust to be robust enough to be connected without denial of service threats.*

The traditional security services are not directly applied on IoT due to the devices run on different platforms and uses different protocols to communicate, especially when the wireless or wire system need to communicate with other devices without human intervention as a machine to machine interaction. There is a need for a new framework to apply the security services on M2M communication architecture.

So a flexible and common security framework is need to be implemented, which deals with security threats in IoT environment. This paper presents detailed information about the security issues related to IoT, and implement a secure framework based Arduino platform to enforce a flexible level of authentication in IoT environment.

Keywords — *Internet of Things; IoT; Embedded Framework; Arduino; Machine to Machine; Machine Identification Threat; Certification Authority; Passive RFID.*

I. INTRODUCTION

Although With the rapidly growing of use Internet - i.e. for sending and receiving email messages, interacting with people via social networking applications, sharing large amount of data, transacting the financial business, playing games, analyzing data and summarizing it and many others -; there are another big area of use Internet begins to emerge as a global platform for allowing the machines, smart devices and electronic objects to communicate, compute and coordinate.

In the middle of 2015, the number of connected devices was around to 4.9 billion, 36% of them are connected things of devices that we use every day (e.g., refrigerators, cars, fans, lights, sprinklers), and "by 2020, the number of connected devices is expected to grow exponentially to 50 billion" [1]. The main driver for this growth is not human population only, the connected things of devices also.

The interconnected things around the world via the Internet, where the humans are interacting with the machines (H2M) and machines are interacting with other machines (M2M), is called the Internet of Things (IoT). The Internet of Things (IoT) can be defined as following: (i) the global network which interconnects smart heterogeneous objects by using Internet technologies (ii) set of supporting technologies such as Radio Frequency Identifications (RFIDs), sensor/ actuators, machine-to-machine communicating devices etc. [2] (iii) combination of application and services using such technologies for business purposes [3]; with focusing on the data and information rather than point-to-point communication. This term was first used in 1999 by Kevin Ashton [2]. The motivation behind IoT is to create Smart city [4] that aimed "create a better world for human beings" by optimize use of public resources, increase the quality of services offered to people and decrease the operational costs of the services, where objects around us know what we like, what we want and what we need and act accordingly without explicit instructions [3].

The IoT depends upon three building blocks, based on the ability of smart objects to be identifiable (anything identifies itself), communicate (anything communicates) and interacts (anything interacts) as in Fig 1.

Beside the challenges that pillars of IoT faced, which related to the connected heterogeneous devices, the speed of connected device identifiability, the scalability and reliability of IoT, the energy optimized for data communication, the localization and tracking capabilities, the self-organization capabilities, semantic interoperability and data management, and more; the security issue is appear as a big challenge of IoT, this is related to support the secure identifiable, establish secure communication and secure interaction to protect connected devices via IoT.

This paper presents detailed information about the security issues related to IOT, and the rest of the

paper goes to implement a secure embedded framework based Arduino platform to enforce flexible level of security and privacy in IoT environment.

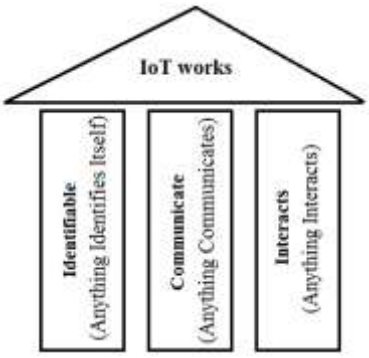

Fig. 1 The three pillars of IoT works.

II. Page Elements of Internet of Things

The Internet of Things (IoT) semantically means a network of interconnected smart things that are uniquely addressable and connected using standard communication protocols; for that the IoT will provide a common environment for heterogeneous smart things to communicate with each other using standardized communication platform. The elements of these common environments will vary depending on the mode of interaction between the things, whether the humans are interacting with the machines (H2M) or the machines are interacting with other machines (M2M) [5].

In general, the main IoT elements should be include the following:

1. Sensing: To gathering (capturing) the information by the biometric, biological, environmental, positional, visual or audible (or all the above) sensors.
2. Communication: To send the captured information for back-end server by network via one of the following communication technologies:
   - Bluetooth, ZigBee, RFID or Near-field for PAN.
   - Wife for wireless LAN.
   - Cellular for wireless WAN.
3. Cloud Based Capture & Consolidation: To provide useful information for the end user (from the gathered data that transmitted previously by sensors) by the back-end server that is a 'cloud based service'.
4. Delivery of Information: To deliver the useful information to the end customer users (either human or another device) using the simple and transparent GUI as possible across multiple device platforms (tablets, smartphones, desktop) and multiple operating systems (iOS, Android, Windows, etc.).

III.M2M Paradigm and Architecture

One of two main modes for IoT that used to interconnected machines around the world via the Internet is Machine to Machine (M2M) mode.

With the increasing number of wireless and smart devices and the exponential increasing need for variety smart applications, M2M refers to technologies that allow both wireless and wired systems to communicate with other devices of the same type without the need of human intervention, while the communications among these devices are known as Machine-to-Machine (M2M) communications [6].

M2M has a wide range of applications such as industrial automation, logistics, Smart Grid, Smart Cities, health, defines etc. mostly for monitoring but also for control purposes. Fig. 2 shows the general M2M communication architecture.

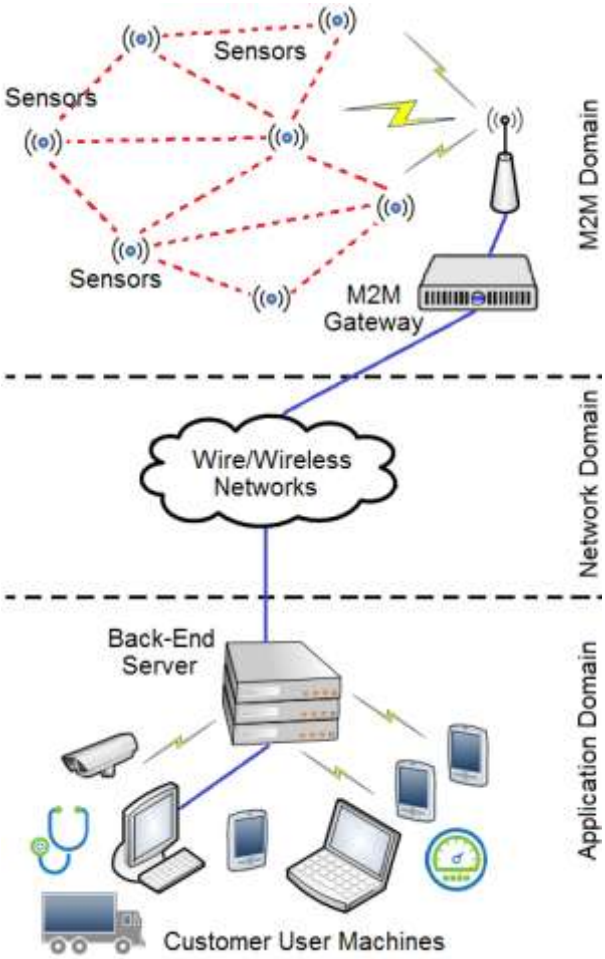

Fig. 2 General M2M Communication Architecture

In the M2M domain, a large number of sensors and M2M gateway are integrated to enable automated and diverse services. Each sensor should be equipped with various functions, such as data gathering, data pre-processing, data storage, distinctive address, wireless transceiver, power supply, etc. They can make intelligent decision and transmit the sensory data packets to the M2M gateway in single-hop or multi-hop manner. While

the M2M gateway is an integrated device using. After collecting the packets from embedded nodes, it is able to manage the collected packets (from sensors) and forwarding them to the remote back-end server via wired/wireless networks [2, 6].

In the network domain, a large number of heterogeneous points of access points that connected to LAN or WAN for sensing data packet transmission from M2M to the application domain. xDSL, Wifi, WiMax, and Cellular communication technologies may be used.

Finally, in the application domain, various real-time services are running by back-end servers to provide useful information for the end customer user devices, such as traffic, logistic, business, home, health, defines, etc. The back-end servers provide useful information that is accessed by user devices indirectly through an installed external application, rather than by server applications. The end customer users devices, mostly for monitoring or control purposes, are used multiple device platforms (tablets, smartphones, desktop) and multiple operating systems (iOS, Android, Windows, etc.).

IV. Security Requirements for M2M Communication Architecture

While IoT are rapidly growing, the threats to the IoT are also deployed. Sensors, the communication between sensors or between a sensor and an access point, M2M gateway, the access points, network and back-end server are potential points for attacks. In order to establish a secure M2M communication architecture, security mechanisms should achieve requirements such as confidentiality, authentication, nonrepudiation, access control, availability, privacy as listed below [1, 7]:

1. Confidentiality ensures that only authorized entities can read M2M sensing data.
2. Authentication allows the back-end server to certify the sensory data of the M2M nodes.
3. Nonrepudiation guarantees that M2M nodes, once sending data, cannot deny the transmission.
4. Access control represents the ability to restrict and control access to the application domain, i.e., it allows only authorized M2M application systems to gain access to the back-end server.
5. Availability ensures that whenever M2M application systems access the back-end server, it is always available.
6. Privacy is very important in the case of privacy-sensitive M2M communication systems.

In general, the cryptographic techniques can be used to achieve confidentiality while digital signature and message authentication code techniques can achieve others. It should be noted that most security mechanisms only efficiently defend against external attacks that launched by attackers who are not equipped with key materials in an M2M communications system, while an internal attack cause more serious damage to the M2M systems compared to the external attacks; for example, the connected malicious things will cause a violation a substantial fraction of the system. The applied of the traditional security services on M2M communication architecture directly represents a big challenge to deal with the internal attack issues in IoT environment due to the devices run on different platforms and uses different protocols to communicate.

V. Arduino Platform

Arduino is an open-source prototyping platform based on hardware and IDE (Integrated Development Environment) for building digital devices and interactive objects that can sense and control the physical world. The Arduino board that called ‘shield’ consists of an Atmel 8-, 16- or 32-bit AVR microcontroller that able to read inputs (i.e. light on a sensor, a finger on a button, or a Twitter message) and turn it into an output (i.e. activating a motor, turning on an LED, publishing something online). While the Arduino IDE are support for C++ to develop embedded systems, each program developed by Arduino is called a ‘sketch’. Arduino started in 2005 as an 8-bit board’s project for students at the Interaction Design Institute Ivrea in Italy as an easy tool for fast prototyping, then changed to adapt to new needs and challenges of IoT applications, wearable, 3D printing, and embedded environments [8].

VI. Embedded Secure Framework

A. Problem Statements

Based on the IoT identification technology, anything can identifies itself, as a smart devices, to communicate and interact with M2M communication architecture, the malicious things will seriously threaten IoT. The malicious device no need to IP spoofing to gain access to IoT, each device can get IPv6 address to connect to the IoT, and the IPSec authentication header was useless. If a single malicious device can identify itself (legitimately) for communicate with other device on IoT, it can violation a substantial fraction of the system, the fake nodes and malicious data, denial of service, impersonation, timing attack, routing threats, side channel attack, phishing attack and more threats can be occur. There is a need for devices trust to be robust enough to be connected without denial of service threats.

On the other side, the memory limitations and processing power, different platforms and different protocols of smart devices considers a big challenge to apply the security services on M2M communication architecture. There is a need for a new framework to apply the security services on M2M communication architecture.

B. Proposed Secure Framework's Aim

The proposed framework that based on Arduino platform aims to enforce the devices trust issue to be robust enough to be connected with M2M communication architecture at the scope of M2M domain. For that the proposed framework enables legitimate smart devices to identifies itself as trust devices and prevents the malicious smart devices for connect with IoT, as shown in Fig. 3.

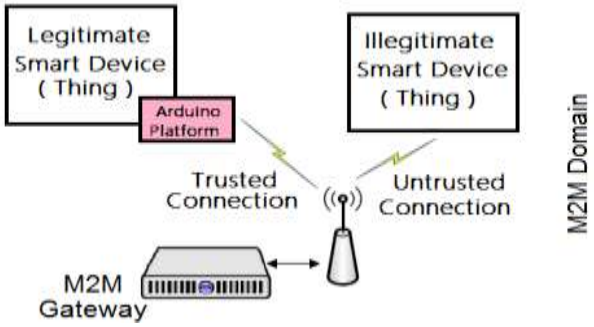

Fig. 3 General Aim of Proposed Secure Framework Architecture

C. Proposed Secure Framework Architecture

The proposed secure framework architecture includes two parts, frozen spots (which includes the basic components that remain unchanged 'frozen' in any instantiation of the framework) and hot spots (which includes the functionality specific to our security issues), Fig. 4 shows the architecture of the proposed framework that works at M2M Domain.

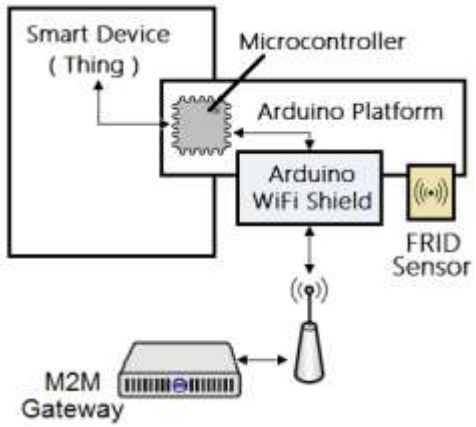

Fig. 4 The Proposed Secure Framework Architecture

The individual components of the proposed secure framework architecture are discussed below:

1. Frozen Spots: To solve the problem of memory limitations and processing power, different platforms and different protocols of smart devices, the proposed framework provides a common platform for smart devices to communicate with IoT. This provides a common framework to apply the security services. The frozen spots part includes the following components.
   a. Smart Devices (Things) that want to connect legitimately for communicate with other device on IoT, those devices may be used to gathering (capturing) the information by the biometric, biological, environmental, positional, visual or audible (or all the above).
   b. Arduino Platform that used as a common platform for reads inputs from the connected smart devices, turn it into an output, run the embedded secure system on its microcontroller.
   c. RFID Sensor that used to receives radio signals from passive tags by scanned the tag from RFID card to retrieve tag (labels attached to the objects to be identified).
   d. Microcontroller that is a hard of the common platform for execute the embedded secure system and the other communication and control instructions.
   e. Arduino WiFi Shield that enables to connect the smart device via Arduino board to the Internet wirelessly.
   f. Wireless Network which operate according to the WiFi technology to connect the proposed framework with the M2M gateway.
   g. M2M Gateway.
2. Hot Spots: To provides a new level of authentication for devices trust to be robust enough to be connected without violating a substantial fraction of the system, the fake nodes and malicious data, denial of service, impersonation, timing attack, routing threats, side channel attack, phishing attack. The hot spots part includes the following components.
   a. Certification Authority that used to make secure connections to a M2M over the Internet. It is an entity that certifies the ownership of a public key (that printed on RFID card).
   b. Passive RFID Checker that check the tag if it's identical with the sorted one or not.

D. Proposed Certification Authority Work Flow

To enforce the secure and robust connection for Smart Devices (Things) that want to connect legitimately for communicate with other device on IoT based the proposed secure M2M communication framework, the procedure of work flow for the Smart Devices (Things) will be as following work-flow flowchart Fig. 5.

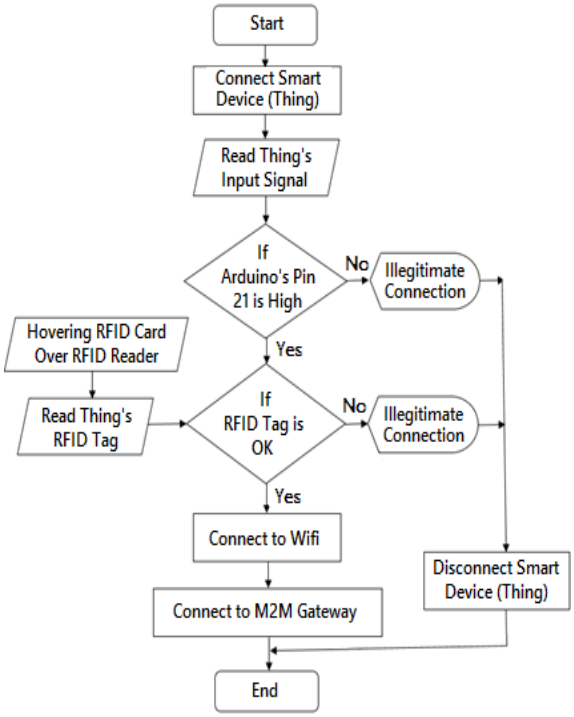

Fig. 5 Proposed Certification Authority Work Flow flowchart

E. Implemented Secure Framework Architecture

The proposed Secure Framework was implemented using the following components:

1. The 'Frozen Spots' part was implemented using the following components beside any connected Smart Devices (Things):
   - **Arduino Mega 2560** with 54 digital input/output pins, a 16 MHz crystal oscillator, a USB connection, a power jack.
   - **ATmega2560 Microcontroller** with RISC architecture to perform up to 16 MIPS as a throughput at 16 MHz.
   - **RFID Sensor** type RC522 communicate using a 13.56MHz. The connected pin layout (based Arduino Mega board) should be as in Table 1.

TABLE I
THE CONNECTED PIN LAYOUT

Arduino Mega Pins	MFRC522 board Pins
5	RST
53	SDA
51	MOSI
50	MISO
52	SCK
With 3.3 V for Power and Shard GND	

   - **Arduino WiFi Shield** that compatible with Uno board and connect to the internet using the 802.11 wireless specification (WiFi).
   - **The connected pin layout** (based Arduino Mega board) will be a compatible layer upon layer.
   - **Fastlink Wireless Network** based 4G technology.
2. The 'Hot Spots' part was implemented using Arduino integrated development environment (IDE) as a cross-platform application and C as a programming language for 'Certification Authority' and 'Passive RFID Checker' components codes.

VII. CONCLUSION AND FUTURE SCOPE

The implemented framework focused on two issues, the first issue is to provide a common platform using Arduino Platform that allow to configuring and coding the common platform to connect smart devices (Things) that run on different platforms and uses different protocols without concern to the memory limitations and processing power of smart devices, this clearly illustrated through the Frozen Spots part. While the second issue is to enforce a level of authentication for smart devices trust to be robust enough to be connected without denial of service threats, this clearly illustrated through the Hot Spots part.

This paper is a new research field which is provide a common secure framework to enforce a flexible level of authentication on M2M communication architecture in IoT environment.

In future, we can replace the RFID Sensor with biometric sensor to add a level of personality-authentication for Certification Authority. Also the cryptographic techniques can be used to add a level of confidentiality for the implemented platform.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito. "The internet of things: A survey". http://blogs.cisco.com/sp/securing-the-internet-of-things-a-proposed-framework, date updated November 10, 2015.

[2] Ovidiu Vermesan and Peter Friess. Internet of Things-From Research and Innovation to Market Deployment. Denmark: Rives Publishers, 2014, 26pp, ISBN (978-87-93102-95-1).

[3] Roberto Minerva, Abyi Biru, Domenico Rotondi. "Towards a definition of the Internet of Things (IoT)". IEEE Internet Initiative, Issue 1, 13 MAY 2015.

[4] Charith Perera and Arkady Zaslavsky. "Improve the Sustainability of Internet of Things Through Trading-based Value Creation". Proceedings of the IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, March, 2014.

[5] Honbo Zhou. The Internet of Things in the Cloud A Middleware Perspective. United States of America: CRC Press, pp.34, 2013.

[6] Zoran Bojkovic, Bojan Bakmaz, Miodrag Bakmaz. "Machine-to-Machine Communication Architecture as an Enabling Paradigm of Embedded Internet Evolution". Recent Advances In Computer Science Proceedings of the 13th International Conference on Applications of Computer Engineering (ACE '14), Portugal, October 30 - November 1, 2014.

[7] Ashvini Balte, Asmita Kashid, Balaji Patil. "Security Issues in Internet of Things (IoT): A Survey". International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015.

[8] Arduino. "Arduino MEGA". Internet www.arduino.cc/en/Main/ArduinoBoardMega2560, date updated November 13, 2015.