Towards the Integration Between IoT and Cloud Computing: An Approach for the Secure Self-Configuration of Embedded Devices

Antonio Puliafito, Antonio Celesti, Massimo Villari, Maria Fazio
DICIEAMA, University of Messina
Contrada di Dio, S. Agata, 98166 Messina, Italy.
e-mail: {apuliafito, acelesti, mvillari, mfazio }@unime.it

***Abstract*—The secure boot up and setup of Internet of Things (IoT) devices connected over the Cloud represents a challengin open issue. This paper deals with the automatic configuration of IoT devices in a secure way through the Cloud, in order to provide new added-value services. After a discussion on the limits of current IoT and Cloud solutions in terms of secure self-configuration, we present a Cloud-based architecture that allows IoT devices to interact with several federated Cloud providers. In particular, we present two possible scenarios, i.e., single Cloud and a federated Cloud environments interacting with IoT devices and we address specific issues of both. Moreover, we present several design highlights on how to operate considering real open hardware and software products already available in the market.**

***Keywords*-Cloud Computing, federation, IoT, self-configuration, security.**

I. Introduction

Internet of Things (IoT) is the next step evolution of Internet, where any physical object/thing having/equipped with computation and communication capabilities could be seamlessly integrated, at different levels, to the Internet. The exploitation of Cloud computing technologies is challenging to support the development of IoT systems, because it guarantees high scalability and reliability of the available services. Thus, IoT and Cloud computing offer new possibilities for sharing data and services through the Internet, by introducing a dynamic global network system with self-configuring capabilities based on standard and interoperable communication protocols.

As highlighted in the *Digital Agenda for Europe [1]*, one of the key challenges for the European Commission is to have a globally competitive Cloud infrastructure for the "Internet of Services" interconnected with "Things" distributed over remote areas. IoT is currently applied in many applications fields, such as in buildings construction, car traffic monitoring, environments analysis, health-care assistance, weather forecast, video surveillances, etc. As a consequence, IoT will offer new services for making cities "Smarter" and it will improve the interaction of people and IoT devices/services with the surrounding environments, increasing the Citizens' quality of life. In these scenarios, security is one of the major factors hampering the rapid and large scale adoption and deployment of IoT and Cloud computing.

There is not limit to the possible scenarios that can be accomplished putting together IoT and Cloud computing. In our opinion, IoT can appear as a natural extension of Cloud Computing, in which the Cloud allows us to access IoT based resources and capabilities, to manage intelligent pervasive environments. In addition Cloud computing can support the delivery of IoT services. Thus an IoT service can be considered as an on-demand Sensing and Actuation as a Service (SAaaS). One of the main problems in deploying IoT devices is the self-configuration of such devices that is necessary to interconnect them over the Cloud.

In our vision, an IoT device should be able to configure itself to interact with the Cloud in a secure way, and should automatically customize its behavior by downloading required features from the Cloud. From the user point of view, when the user turns on his/her IoT device and connect it via WiFi (or other communication technologies), he/she has just to wait for the self-configuration of the device and, then, can start to use it.

In order to self-configure IoT devices in a secure way and allowing them to interact over the Cloud, devices should be equipped with capabilities including security keys, cryptographic algorithms, hidden IDs, etc. This approach is already a reality. An example is represented by *my-devices.net*, that is a Cloud provider delivering secure remote access services to embedded devices via HTTP(S) or other TCP-based protocols. As well, *Temboo* [1] provides innovative commercial solutions to interconnect IoT devices with Cloud services (e.g., Storage, Processing, Messaging, etc.) using simple Application Program Interfaces (APIs). These examples represent only "a few drops in the ocean of IoT and Cloud computing", due to the great interest of research and business companies in this application field.

In our previous work [2], we analyzed current issues on the self-configuration of IoT devices connected over the Internet to Cloud providers. Specifically, we proposed a secure approach for the boot up and setup of embedded devices. In this paper, we discuss how to apply our solution in real environments, presenting two possible scenarios: a single Cloud and a federated Cloud environment interacting with IoT devices. Moreover, we present several design highlights, discussing how to operate considering real open hardware and software products already available in the market. The solution proposed hereby is aimed at IoT enterprises that consider Cloud computing strategic to

[1] https://www.temboo.com

improve their business.

The rest of the paper is organized as follows. Section II discusses related works. Section III presents two challenging scenarios integrating IoT and Cloud computing. In Section IV, we discuss the main factors involved for a secure self-identification of IoT devices. In Section V, we propose an IoT Cloud-Based architecture. In Section VI, we discuss how IoT devices joing the Cloud system can self-register themselves to perform a self-configuration process. Section VII concludes the paper.

II. Related Works

Security in IoT and Cloud computing is a widely discussed topic that hardly influences he rapid and large scale adoption and deployment of such technologies [3], [4].

In [5], the authors investigate security issues and challenges on IoT-based Smart Grids (SG), and define the major security services that should be considered when dealing with SG security. An approach to simultaneously scan several IoT objects in a short time is presented in [6]. The authors present the notion of Probabilistic Yoking Proofs (PYP) and introduce three main criteria to assess related performance: cost, security, and fairness. The proposal combines the message structure of classical grouping proof constructions with an iterative Poisson sampling process where the probability that each object is sampled varies over time. A Key distribution approach for secure e-health applications in IoT is presented in [7], where the authors conduct a formal validation of security properties. A secure mutual authentication scheme for an RFID implant system is presented in [8]. The authors propose a scheme that relies on elliptic curve cryptography and the D-Quark lightweight hash design. The D-Quark lightweight hash design is tailored for resource constrained pervasive devices, considering costs and performance. The computational performance analysis shows that the proposed solution has 48% less communication overhead compared to existing similar schemes. In [9] the authors propose a secure and scalable IoT storage system based on revised secret sharing scheme with support of scalability, flexibility and reliability at both data and system levels. Shamir's secret sharing scheme is applied to achieve data security without complex key management associated with traditional cryptographic algorithms. The original secret sharing scheme is revised to utilize all the coefficients in polynomials for larger data capacity at data level. In [10], the author propose an approach to provide secure IoT services using the Datagram Transport Layer Security (DTLS) as the de facto security protocol. In particular, they examined problems in applying the DTLS protocol to IoT, which comprises constrained devices and constrained networks. To solve such problems, they separate the DTLS protocol into the *handshake phase* (i.e., establishment phase) and the *encryption phase* (i.e., transmission phase). An overview of the main security challenges in IoT-aided robotics applications is presented in [11], that is specifically focused on network security. In [12] the authors investigate the possibility to unify resilient Cloud computing and secure IoT in Smart Cities scenarios. Considering the self-configuration issue of IoT devices in a Cloud computing scenario, in [13], the authors present an interesting IoT Cloud architecture exploiting Arduino devices, whereas in [14], the authors propose an IoT service provisioning using a Cloud computing system. However, both [13] and [14] lack of secure self-configuration mechanisms during the boot up phase. In fact, they require human interactions and an a priori configuration of devices. In this paper, we try to overcome this gap.

III. Single and Multi Cloud Scenarios for IoT

In this Section, we present two challenging scenarios, that we respectively identifies as"Single-Cloud" and "Multi-Cloud" (see Figures 1 and 2). Both the scenarios include different users holding several IoT embedded devices connected to Internet (e.g., through a domestic WiFi network). Each device is able to automatically configure it-self downloading its configuration from a given Cloud provider. As shown in Figure 1, in the Single-Cloud scenario, several datacenters belonging to a Cloud operator are spread over the world. For example, Datacenter A is placed in USA, datacenter B is located in Europe, and datacenter C is placed in Asia. Each datacenter collects data coming from IoT embedded devices connected in the geographical area that it serves. The Multi-Cloud scenario shown in Figure 2 is much more challenging than the previous one, because datacenters belong to different cooperating Cloud providers. In the example, Cloud B is a device manufacturer, whereas the Cloud A and C are IoT service providers. Cloud A, B and C establish a federation relationship with the objective to improve their business. An interesting question is how to establish agreements among these Clouds. Cloud B can provide different kinds of services to its customers but also to Cloud A and C that provide IoT services. In addition, Cloud B can be the third-party entity responsible to certify the goodness and trustiness of its IoT devices. A similar situation already takes place in trusted computing considering the Trusted Platform Modules (TPMs) endorsed in motherboards by manufacturers. At the beginning, Cloud A and B make an agreement for a Single-Sign-On service. When an IoT embedded device wants to access the Cloud A, it has to perform an authentication on Cloud B. If the authentication succeeds, Cloud A will trust Cloud B. Thus, Cloud A will complete the registration of the device. After that, Cloud A and B establish a federation relationship. To this aim, Cloud B (i.e., the device manufacturer) tracks each IoT embedded device in terms of firmware version, bug reporting, etc, thus to be able to authenticate it without knowing nor the real location of the device neither its owner. Cloud A (i.e., IoT service provider) can be notified from Cloud B. Cloud B needs to identify the device without exchanging users' data and device Media Access Control (MAC) addresses.

In Figure 2, the federation agreement for SSO can be further extended implementing additional mechanisms for interoperability among Clouds. According to the reference scenario, each user gathers data coming from his/her embedded IoT devices by means of a Cloud's web portal and stores them into the Cloud. To manage such Big data, different types of information from different providers have to be processed. For

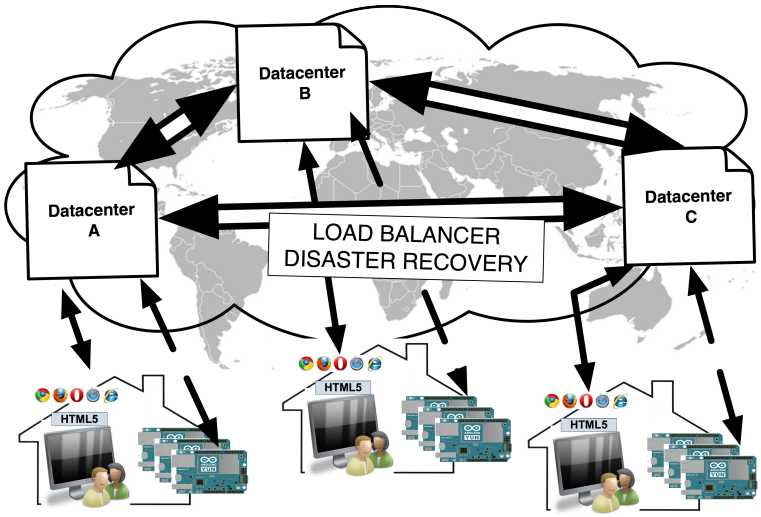

Fig. 1. Single-Cloud Scenario with one cloud operator distributed among more sites, IoT devices, and Customers.

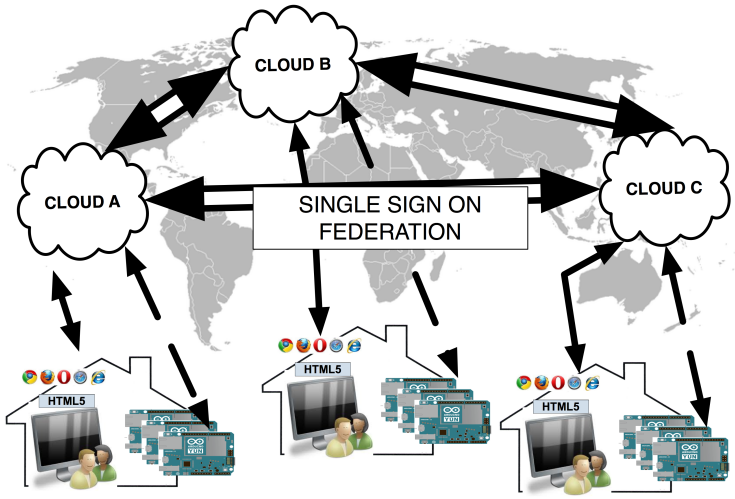

Fig. 2. Multi-Cloud Scenario with more Cloud operators, IoT devices, and Customers.

example, to provide a seamless service to the user, Clouds A and B should manage the following information:

- devices information on Cloud B;
- user authentication, authorization, and accounting information on Cloud B;
- devices configuration for initial setup on Cloud A;
- devices configuration for life-cycle operations on Cloud A;
- devices sensed data on Cloud A;

To store and manage all these data in a scalable way, every Cloud should host a local distributed database. In a shared and opportunistic configuration of Clouds belonging to a federation, it is also possible to think about a global database distributed among different federated domains, which works as a global big catalogue holding information for users and devices (e.g., login, keys, code, IDs, MAC repository, etc.).

IV. Towards Secure Self-Identification of IoT Devices

This Section, we discuss how existing IoT embedded devices might be extended and used to carry on self-identification in the scenarios previously described. Specifically, IoT devices should be on-boarded with Security Keys, Cryptographic Algorithms and Hidden IDs (hIDs). Thus, we analyze a well-known IoT platform (that is Arduino Yun [2]) in order to discuss the effectiveness of self-identification mechanisms.

A. Arduino Yun

The Arduino open hardware framework is a consolidated architecture able to fulfill IoT requirements especially for its cheapness and simplicity of utilization. Many versions, shields, and extensions exist over the market for the Arduino platform. Among them, Arduino Yun is the framework able

[2]

to provide Arduino capabilities along with Linux embedded features. Specifically, Yun is different from the other Arduino boards because the ATmega controller communicates with the Atheros AR9331 processor. The latter supports a Linux distribution based on OpenWRT named Linino, offering a powerful networked computer with the easiness of Arduino.

Figure 3 shows the Yun architecture. The left side of the picture depicts the Arduino part, whereas in the right side the Linino part is shown. Yun has built-in WiFi/Ethernet boards that provide communication capabilities. In our scenarios, Linino can be used to accomplish security features and to perform the interactions with the Cloud. In particular, Webclient (i.e., Curl), XMPP client, Python and OpenSSL can be easily developed on this device for interacting with other devices and with the Cloud in secure way.

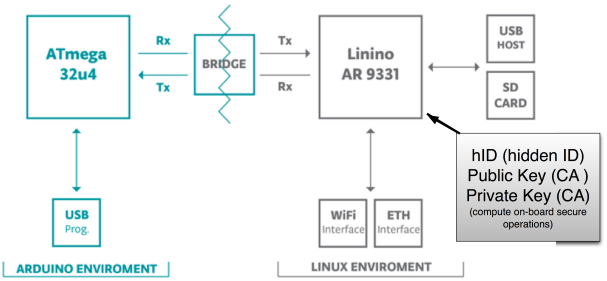

Fig. 3. Arduino Yun extended with secutity capabilities.

B. Security Keys, Cryptographic Algorithms and Hidden IDs

In order to achieve the scenarios discussed in Section III, an IoT device such as Arduino Yun should be equipped with a new component mounted on the board by the manufacturer and offering several security capabilities. In particular, these security capabilities should include: Security Keys (e.g., a couple of public/private keys X509v3 based (K_{pub}, K_{priv})), Cryptographic Algorithms, a hidden ID (hId). The *hID* is a numeric serial-number used by manufacturer for recognizing each board. It is hidden because no one must read it. Here, we introduced the concept of Obfuscated ID (obH) derived from the MD5 hashing function. The major property of an hashing function is its incontrovertibly, in fact it is also defined an one-way function (i.e., from the output of an hashing function it is not possible to deduct the input). Hence, obH is useful to track boards hiding information on public MAC addresses and board owners:

$$obH = hash(hID, MAC) \quad (1)$$

obH represents a board index does not provide sensitive information on the board itself and, hence, can be stored in whichever public database. In any communication between the device and the Cloud operator (e.g., Cloud A in Figure 2), a Message (M) should be included in the body of all communications concatenating obH, MAC, and a public key K_{pub} to implement secure communications.

$$M = concat(obH, MAC, K_{pub}) \quad (2)$$

The signature mechanism based on the public key K_{pub} guarantees the trustiness of the sender. K_{pub} is assigned at the production stage by the Certification Authority (CA) of the manufacturer of the IoT device. On the contrary, the private key K_{priv} is not accessible externally from the chip embedded in the device, but it can be used by internal security algorithms:

$$SM = signature(K_{priv}, M) \quad (3)$$

C. Adding Secure Hardware Capabilities

Trusted Computing (TC), defined by the Trusted Computing Group (TCG) [15], combines hardware and software security mechanisms to enhance the security level of computing environments. The main goal of TC is to provide stronger security than the traditional software-based security systems and to enforce the integrity of a system when it interacts with other ones. The distinguishing feature of TC is the incorporation of Roots of Trusts (RoT) that aims to perform specific functions in a secure way, such as measurement, storage, reporting, verification, and/or update. TC implies the adoption of an hardware chip called Trusted Platform Module (TPM), that is able to provide RoTs and to extend trust to the other parts of the device by building a chain of trust. It offers facilities for the secure generation of cryptographic keys and it is capable to perform platform authentication, since each TPM chip has an unique and secret RSA key burnt into as it is produced (i.e., the Endorsement Key (EK)). The TPM includes capabilities such as machine authentication, hardware encryption, signing, secure key storage and attestation. Born for securing traditional Personal Computers, the TCG is currently looking at both embedded and mobile devices whose reference architecture specification drafts were released respectively in April and June 2014. The specifications provide guidelines on how to onboard the TPM in a device even though there have not been so many implementations yet on real harware devices. TC and embedded systems are at the early stage, however, in our opinion, TC is a valid soluting to develop harware security capabilities in IoT devices interacting with the Cloud.

V. An IoT Cloud-Based Architecture

In this section we describe an IoT Cloud-based architecture that is able to support the self-identification on secure communications, as described in the previous sections. To this aim, we specifically refer to the CLoud-Enabled Virtual EnviRonment (CLEVER), a secure Message-Oriented Middleware (MOM) able to support federated Cloud services developed in oru labs [16]. CLEVER sets up a Cloud system able to manage both sensing and virtualization services using the XMPP protocol. In addition, the middleware supports big data management by means of the NoSQL database MongoDB. Figure 4 shows our IoT Cloud-Based Architecture that supports both single Cloud and Multi-cloud scenarios. The infrastructure needs to rely on virtualization platform for guaranteeing a high degree of flexibility and elasticity through Virtual Machines (VMs). All the Physical Machines (PMs) are equipped with a piece of CLEVER middleware for the cluster managements. The circle

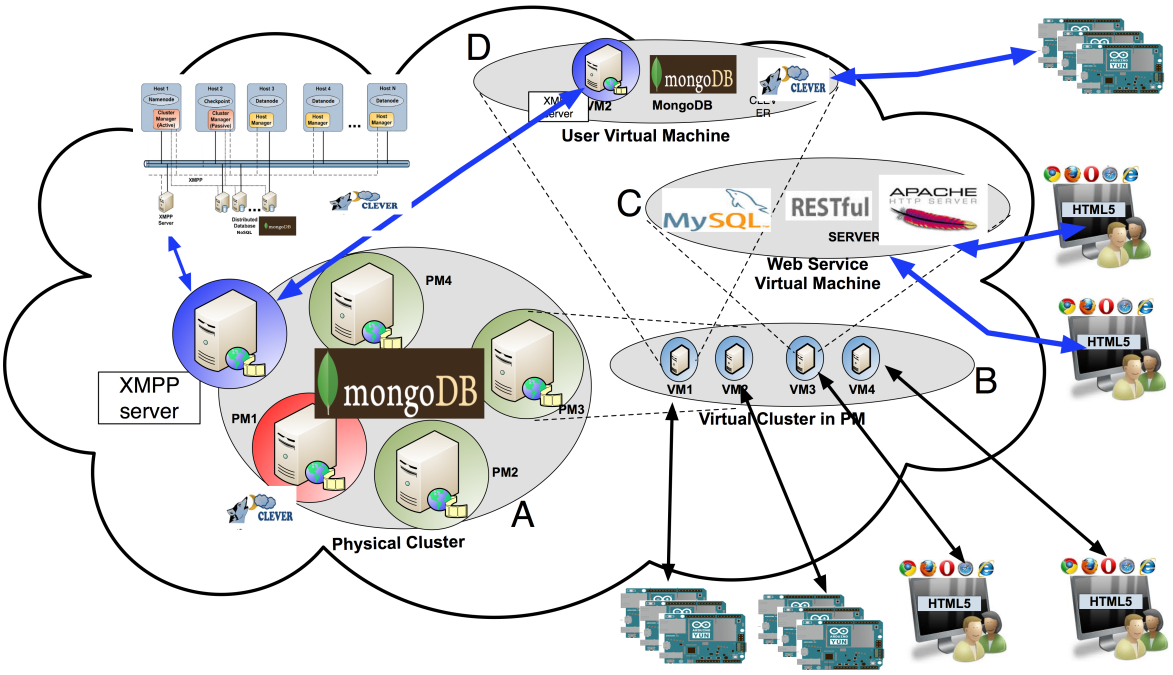

Fig. 4. Example of IoT device manufacturer managing its own datacenter using our architecture. The Figure shows several web clients and IoT devices extended with security capabilities interacting with a Cloud system arranged using CLEVER.

shape with the label A represents the cluster where virtual instances of IoT services are lunched. The Cloud is aimed at the maintenance of the current solution but also for customers management. In the distributed instance of MongoDB, information on IoT obH, device status (e.g., firmware version, on-board add-ons, etc.) and the data devices collect are stored. The XMPP server setup bidirectional bus channels. The ellipse shape with the B label highlights the execution of several VMs into a PM. Each VM contains different services and interacts with different customers and devices. Shapes with C and D labels show possible services, such as Apache, MySQ, PHP services, VMs with a minimal version of CLEVER, the XMPP server and MongoDB. The D shape represents a container in which sensed data are stored and confined inside a VM. Many IoTs, having the XMPP client, are dynamically assigned (after the first contact with the secure webclient) to the XMPP server deployed into the VM. Many customers (since with their IoTs) can rely on the same VM. This service can scale up and down in relation to the number of Customers and IoTs. Shape C represents the main web portal service used for customers, and for making MAC-Users associations. Even it, can scale up and down respect to the number of customers.

A. Arranging a Cloud Systems Using CLEVER

As depicted in Figure 5, each CLEVER cluster includes several PMs organized in a cluster. Each PM is controlled by a management module, called Host Manager (HM), and only one PM runs a cluster management module, called Cluster Manager (CM). CM acts as interface between Cloud clients (e.g. IoTs, applications, web services and end-users exploiting Cloud resources) and software agents running on PMs. CM receives commands from clients, gives instructions to HMs, elaborates information and finally sends back results to the clients themselves. It also performs tasks for the management of Cloud resources and the monitoring of the working state of the cluster. A CM is elected among all the HMs using a distributed *self election protocol* and it works in the ACTIVE mode. A second CM is also elected as backup, but it is configured in the MONITORING mode. The MONITORING CM is not involved in the cluster management, but it keeps a synchronized copy of the internal state of the ACTIVE CM, hence, it is able to set up all the active services if the ACTIVE CM fails. To make easier our dissertation, from now on, we refer to the ACTIVE CM just as CM.

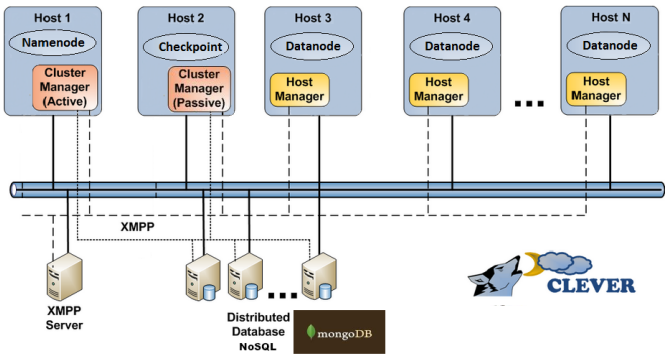

Fig. 5. In Datacenter Generic Architecture of CLEVER.

Communications among distributed components into a CLEVER Cloud are based on XMPP, due to its flexibility and high level of re-activeness. A Jabber/XMPP server provides basic messaging, presence, and XML routing features within

the Cloud. All the PMs in the Cloud are connected via the Multi User Chat (MUC) labeled *Main Room* and cooperate according to the CM orchestration directives. A MUC, identified as *Shell Room*, allows clients to submit their requests and receive the service. Due to the cluster-based architecture of CLEVER, only CM and clients access the Shell Room. These two communication channels are shown in Figure 5 as thick black lines.

To set up a federation, CMs belonging to different Clouds exchange messages through the MUC identified as *Federation Room*, and only CMs of federated Clouds access it. MONITORING CMs cannot enter the Federation Room, since they are not directly involved in resource management.

The XMPP server necessary to establish the federation, and, hence, to manage the Federation Room, can be entrusted by a third part entity, which set up a Jabber Server out from the domains of Cloud providers, only to fulfill federation requirements. Since the MUC can be accessed only by components into federated domains, it is necessary to check for their credentials. To avoid a priory static configuration of accounts into the XMPP server, the third part entity has to authenticate component credentials. To this aim, XMPP federation capabilities can be exploited. The third part entity does not need to maintain the credentials of all CMs involved in the federation, but a trustiness agreement among all the Jabber Servers allows to setup an XMPP federation where sharing authentication artifacts (tokens).

B. Interaction of IoT Devices with the Cloud: a Hybrid Approach

In this Section, we discuss a hybrid approach for allowing the IoT device to interact with a Cloud system, e.g., arranged by means of CLEVER. To describe the interaction approaches, we refer to two possible cases:

- Case A: we consider the "simplified" scenario, where the device manufacturer coincide with the Cloud operator (i.e., Cloud B), hence it has a full control over the board with bidirectional XMPP communications.
- Case B: we consider the "challenging" scenario, where the device manufacturer (i.e., Cloud B) makes an explicit full agreement with the Iot service provider (i.e., Cloud A) and both belong to a Cloud federation. In this scenario, Cloud B offers theis Plaftorm as a Service (PaaS) to other Clouds (e.g. XMPP server, authentication system, NoSQL database, etc.). Two chat-rooms are preconfigured, between the XMPP client of the IoT device and the XMPP client of the Cloud provider: the first one is used for firmware deployment and bug management. the device manufacturer (i.e., Cloud B) such a communication system to communicate with the IoT device. Cloud A can join this communication. The second chatroom is used for sending sensed data: the IoT service provider (i.e., Cloud A) such a communication system for its purposes, but Cloud B cannot hear the communication, if an encrypted channel is used.

This hybrid interaction approach includes two different types of client running on IoT devices tahta operate at different stages: a web client for secure RestFul communication ans and the XMPP client for bidirectional communication.

1) RESTFull Web Client: The main idea is to use the web client after the first association of an IoT device with its Home WiFi network. Thus, the web client accesses Internet and contacts the default web server of its Cloud provider using the https protocol. The IoT device, such us Arduino Yun, using its private key performs a challenge-response process to perform a SSL mutual authentication with the web server, and if it succeed, the IoT device sends a message M (see the Equation IV-B) in a JSON document's body to the web server. Thus, the IoT device is recognized and bind to the service. The Secure web client is used only at the beginning for the simplified scenario. After that the message M is sent, the web server at the Cloud of the manufacturer takes the control of the IoT device and can perform the subsequent actions using the XMPP protocol.

2) The XMPP Client: It allows to simplify the interaction among the IoT device and severl Cloud providers, especially in the "challenging scenario". Considering such a scenario, let us assume that the Cloud A (the IoT service provider) needs to setup two elements, i.e., a SD card to plug into the IoT device and a web service. The SD card contains data for accessing Cloud A (e.g., the URI and the public certificate of the CA). The web service is able to perform a SSO authentication, redirecting a request to Cloud B for getting authentication tokens. Hence Cloud B (the device manufacturer) and Cloud A (IoT service provider) are both in charge to finalize the step of early device identification. The XMPP protocol was originally designed for efficiently managing messages among peers over the Internet. The nature of XMPP allows to transparently gain the access over the Internet, using mechanisms of firewall pass-through, without any user intervention, establishing bidirectional communications. It is based on the XML standard, hence it is rather simple to be extend for enforcing security and signing mechanisms. In addition, it is possible to accomplish signature and encryption of XML messages leveraging public/private keys. Any device with the OpenSSL stack can use such functionalities. The XMPP client, starts it execution after that the interaction of web client successfully ends. This XMPP client can be used both in the simplified and challenging scenarios.

VI. Registration Strategies of IoT Devices Joing the Cloud

The IoT device, e.g., the Arduino Yun extended with security capabilities, can follow two different registration methods:

- Unsupervised: auto registration of MAC address and obH;
- Supervised: end-user web registration of MAC address and obH.

In both cases, the end-user needs to enable the IoT device (e.g., the Arduino Yun board) to maintain the WiFi network association using the wps button on his wireless AP. Hence, the IoT device can access the Internet performing the authentication as describe in Section IV. In the Supervised case, the IoT device board flashes an orange LED, and after its

partial registration it shows an orange fixed-on LED. The full registration is achieved when the end-user associates the IoT device board with his/her web profile. The users adopts a web site to register the board, in particular typing the MAC address shown in the external part of the box provided by the manufacturer. If the MAC in M matches the MAC typed in the website, the board flashes a green LED, and the user can confirm the operation, otherwise (obtaining no flashing LED) he/she should repeat the procedure. After that, the full registration has been accomplished, the board shows a green fixed-on LED. Now the Cloud has the full control of the board, hence it can deploy firmware, managing configuration, install software and so on. The user only pushed a button (wps) and typed a code in the web site of the Cloud operator.

The solution proposed can follow two main version branches. The early version is strongly bound with the device manufacturer (i.e., Cloud B) that it is in charge for the following tasks: i) pre-programming the IoT device, ii) updating the firmware, and iii) releasing new applications. The second version looks at situations in which the device manufacturer is in charge for task i), whereas the other IoT service providers (i.e., Cloud A and C) are able to deal with tasks 2 and 3. These tasks are possible if Cloud IoT service providers establish an agreement with the Cloud acting as device manufacturer. Cloud acting as IoT device manufacturer have to equip IoT device with SD card to achieve such a scenario. Thus, our idea is to leverage the Single-Sign-On concept for allowing a device to make a registration on a Cloud IoT service provider, interacting with the Cloud acting as IoT device manufacturer. When the IoT device is able to establish a connection, it reaches Cloud IoT service provider, hence its service operates a redirect to the Cloud IoT device manufacturer, that act as Identity Provider, for verifying the obH message with its Signature. If the Cloud manufacturer recognizes the device, it releases a token, hence the Cloud IoT service provider can complete the Unsupervised registration. The Supervised registration is performed by end-users that can initially follow the same approach. To accomplish this scenario, the Cloud IoT service provider needs to make an explicit agreement with the Cloud IoT device manufacturer for understanding how to interact each other. The obH message cannot allow the device manufacturer Cloud to know detailed info about the board. However, it can track its general status, firmware version, bugs, and so on.

VII. Conclusion

In this paper, we discussed an approach to integrate the IoT with Cloud computing. In particular a system is presented analyzing the different elements involved and how they interact with each other. Using the Arduino Yun as example, we discussed how IoT devices can be extended to support the interaction with the Cloud. In particular, we focused on a system that allows a Cloud provider to deploy the firmware and configure the device, and on one hand to perform sensed data transfer from the device to the Cloud provider. In the end, we discussed how the overall system works, also presenting two possible Cloud scenarios. Currently, IoT devices are at the early stage and how argued in this paper, they are not ready yet to support complex Cloud scenarios, even though the roadmap toward innovative Cloud IoT services begins to be tracked.

References

[1] Unleashing potential of Future Internet and Cloud computing, http://ec.europa.eu/digital-agenda/en/news/unleashing-potential-future-internet-and-cloud-computing November 2013.

[2] M. Villari, A. Celesti, M. Fazio, and A. Puliafito, "A secure self-identification mechanism for enabling iot devices to join cloud computing," in *First International Conference on Safety and Security in Internet of Things (SaSeIoT)*, October 2014.

[3] Y. H. Hwang, "Iot security & privacy: Threats and challenges," in *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security*, IoTPTS '15, (New York, NY, USA), pp. 1–1, ACM, 2015.

[4] Z.-K. Zhang, M. C. Y. Cho, and S. Shieh, "Emerging security threats and countermeasures in iot," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '15, (New York, NY, USA), pp. 1–6, ACM, 2015.

[5] C. Bekara, "Security issues and challenges for the iot-based smart grid," *Procedia Computer Science*, vol. 34, no. 0, pp. 532 – 537, 2014. The 9th International Conference on Future Networks and Communications (FNC'14)/The 11th International Conference on Mobile Systems and Pervasive Computing (MobiSPC'14)/Affiliated Workshops.

[6] J. M. de Fuentes, P. Peris-Lopez, J. E. Tapiador, and S. Pastrana, "Probabilistic yoking proofs for large scale iot systems," *Ad Hoc Networks*, no. 0, pp. –, 2015.

[7] M. R. Abdmeziem and D. Tandjaoui, "An end-to-end secure key management protocol for e-health applications," *Computers and Electrical Engineering*, 2015.

[8] S. R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho, "An elliptic curve-based mutual authentication scheme for {RFID} implant systems," *Procedia Computer Science*, vol. 32, no. 0, pp. 198 – 206, 2014. The 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), the 4th International Conference on Sustainable Energy Information Technology (SEIT-2014).

[9] H. Jiang, F. Shen, S. Chen, K.-C. Li, and Y.-S. Jeong, "A secure and scalable storage system for aggregate data in iot," *Future Generation Computer Systems*, vol. 49, no. 0, pp. 133 – 141, 2015.

[10] H. K. Namhi Kang, Jiye Park and S. Jung, "Esse: Efficient secure session establishment for internet-integrated wireless sensor networks," *International Journal of Distributed Sensor Networks*, pp. 133 – 141, 2015. Hindawi.

[11] L. Grieco, A. Rizzo, S. Colucci, S. Sicari, G. Piro, D. D. Paola, and G. Boggia, "Iot-aided robotics applications: Technological implications, target domains and open issues," *Computer Communications*, vol. 54, no. 0, pp. 32 – 47, 2014.

[12] G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G. Todoran, and V. Suciu, "Smart cities built on resilient cloud computing and secure internet of things," in *Control Systems and Computer Science (CSCS), 2013 19th International Conference on*, pp. 513–518, May 2013.

[13] A. Chandra, Y. Lee, B. M. Kim, S. Y. Maeng, S. H. Park, and S. R. Lee, "Review on sensor cloud and its integration with arduino based sensor network," in *IT Convergence and Security (ICITCS), 2013 International Conference on*, pp. 1–4, Dec 2013.

[14] M. Aslam, S. Rea, and D. Pesch, "Service provisioning for the wsn cloud," in *Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on*, pp. 962–969, June 2012.

[15] Trusted Computing Group (TCG): http://www.trustedcomputinggroup.org.

[16] A. Celesti, M. Fazio, M. Villari, and A. Puliafito, "SE CLEVER: A Secure Message Oriented Middleware for Cloud Federation," in *IEEE Symposium on Computers and Communications (ISCC 2013)*, (Split, Croatia), July 7 2013.