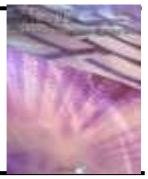
DSR Design for Scientific RENAISSANCE



New Security Approach for IoT Applications as a Cloud Services

Ali Hussein Shamman Wael Jabbar abed Al-nidawi
Zaid Farooq Salih Saba Kamil Jaafar Al-wassiti

Almustaqbal University College[1.2], Universiti Kebangsaan Malaysia[3,4]

alial-safi@mustaqbal-college.edu.iq

Dr.WaelAl-nidawi@mustaqbal-college.edu.iq

zaid.iphone0@gmail.com

p103496@siswa.ukm.edu.my

ISSN (Printed): 2314-7350
ISSN (Online): 2231-8852

Abstract

Integration IoT applications and cloud services that are appearance in the pioneer IT solution, is a most important issue in the current research. IoT is a preferable technology that is following different ways in produce and lunch about things (*sensors, devices or machines*) such that communicated together under an advanced network. Also, cloud computing (CC) has the new approach for IT resource management and the new platforms for service development, when a broad access network is available. Therefore, IoT and cloud computing (CC) should be considered as two critical paradigms about IT *resources, services and things* under large access interconnections and ubiquitous networkaccess.

Aggregation of cloud computing (CC) and IoT technologies, which we write CCIoT as its acronyms, may be a revolution in the future of the IT utilization, so much different from which we have seen in the past decades. This fact is happened when their multi research lines will be succeeded. In this regard, we need to response to the main research parts: 1) advanced smart things in the CCIoT terminals, 2) decentralized and live communication interof things, 3) unlimited resource with access facilitated, and also 4) high security where is divided in the four subjects: *data access and protection, things management, secure CCIoT interconnection protocols for devices,* and *services monitoring*.

In this research we will study CCIoT security aspects for deterministic problems. At first we have review and select a best configuration for an IoT application where hosted to the cloud platform. Then we redefine our security problem where is confined for some functions. For improve these functions we implement new proposed methods where it maybe cover one or

more security threat. The result of our work will be comparing to the other ways and carefully reported. Result of this research may be useful in the part of proposed secure configuration of Cloud and IoT when they are provide common service and also improve security functions resistance.

Keywords: IoT application, cloud services, PMIPv6, KMIP, Barbican.■

1. IoT and Cloud for Service development

- Internet of Things (IoT)Services
- Cloud Computing (CC)Platforms
- IoT and Cloud Aggregation
- Security Challenges

Information technology (IT) progress is related to provide the new services and infrastructures that will be used for many applied systems. Internet of things (IoT) and cloud computing (CC) follow this trend of IT progress with specific approach. IoT consist of different ways in *produce and lunch about things (sensors, devices or machines)* such that communicated together under an advanced network. And cloud computing (CC) has the new approach for *IT resource management and the new platforms for service development*, when a broad access network is available. Now, the convergence between cloud computing (CC) and internet of things (IoT) has become a hot topic for research in the last years. An IoT service would have enabled with distributed nature of infrastructure in the cloud computing (CC). So, in this research we proposed a new configuration for integrate the cloud computing (CC) and IoT technologies, which we have called CCIoT asacronyms.

In the CCIoT configuration we response to problems where have correlate to integrate conditions. First we describe a future for advanced smart things that are the CCIoT terminals, which will be capable for interconnection with together. Next, the CCIoT facilities for decentralized management of live communication inter of things, will be discussed. At continue define solutions for unlimited resource where has accessible facilitated. Now we engage to the CCIoT security gaps somehow that curb threats. We know as well as the security subjects of this integration is the most critical part of such configuration.

A comprehensive review of CC and IoT services has been shown that we have more challenges with security aspects as *data protection and information confidentiality*. Our investigated on security solution of CC services and IoT applications separately and also together has been shown that: security issue for CCIoT is divided in the four subjects: *data access and protection, things management, secure CCIoT protocols for interconnection and network access, and services monitoring*. In this regards we have some security issues:

- **Confidentiality**: IoT and cloud computing are relies to increment of data shearing in

inter of device or their network connections. This massive data transmission can make more security threat about data confidentiality and dataprotection.**Data Less**: In the CC we have live migration that allows a VM to be moved from one host to another while the guest IoT smart agent is running, so we will have low management on the data and users that for example data less may be happened.

- **Secure Channel**: There is many configuration and protocol for connection cloud platform and IoT service, where has different stability of security conditions. For example user or agent identification, action or access authorization, interaction to the other users or agents and thingsaccess.
- **Big Data and Things**: In the CCIoT, we have faced to the so many IoT agents where cause to ubiquitous network access and Big Data about information of traffic of channels, where is increased amount of security threat. For example in the IoT service we have multi-user access to a thing (*sensor, device or machine*) where need to different permissionprotocol.

These security issues of cloud computing are impending for its widespread adoption and managed the IoT services. So, control of user or things, data and applications under these assumptions for an IoT service in a cloud platform is more sophisticate. In this research thesis we have decide to follow security methods for an IoT service when has managed (*integrated or connected*) in a cloud environment. Now, our work should be addressed in the two aspects;

- **Configuration**: Study *a secure configuration* for an IoT service when is hosted in the cloud platform. For aspect of data shearing inter IoT agent and cloud virtual machine, which has high degree of securityparameters.
- **Data**: Proposed a new method for cloud data protection and data confidentiality consist of *advanced key-exchange for packetsencryption*.

This thesis is organized as follows: At first we will define our configuration for CCIoT and study their security aspects for some deterministic problems. In this phase we have review and select a best configuration for an IoT application where hosted to the cloud platform. Then we redefine our security problem where is confined for some functions. For improve these functions we implement new proposed methods where it maybe cover one or more security threat. The result of our work will be comparing to the other ways and carefully reported. Result of this research may be useful in the deployment of secure configuration of Cloud and IoT when they are provide common service and also improve security functions resistance.

1.1. Internet of Things (IoT)Services

IoT service has been considered as an interconnection of smart devices where has been activated on a software applications for example a data sharing software [23]. An IoT service distinctly will be defined as a data shearing, based on wireless network, where is implemented with proxy mobile IP (PMIP) protocol or the other similar network protocols as IETF, URI, TCP/IP, UDP and etc. we gather all protocols where proposed for IoT services inthe

IoT is a latest technology where is following different ways in produce and lunch about things (*sensors, devices or machines*) such that communicated together under an advanced network. An overall architecture of IoT technology parts is shown in figure 2. The Internet of Things (IoT) is consist of physical objects as *mobile, devices, vehicles, buildings* and other items which are embedded with seteped with IoT software, sensors, and network connectivity protocols where can to gather and interchange data with the cloudcenters.

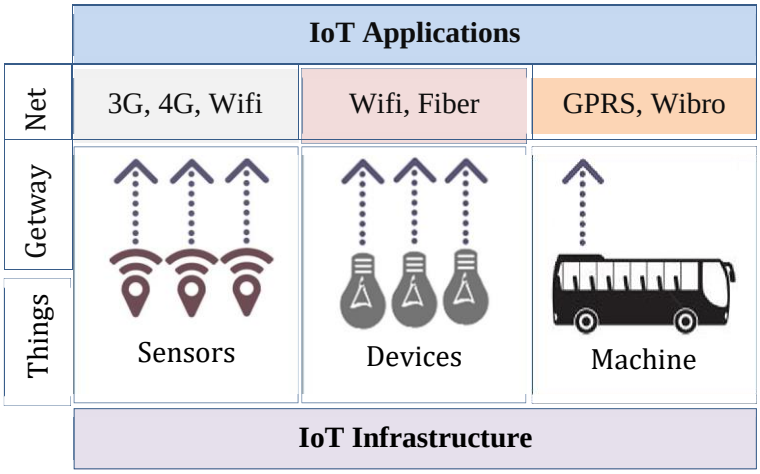


Figure 1. IoT Architecture

So, the IoT paradigm relies on the identification and use of a large number of heterogeneous physical and virtual objects (i.e. both physical and virtual representations), which are connected to the Internet [24]. A briefly description for the IoT parts is:

- IoT Infrastructure: it is consist of *1) internet infrastructure and 2) uniquely identifier code for any things when they are more than 30 Billion things, 3) Uninterrupted electrical energy for things* [25].
- IoT Thigs: *we have three part of things 1) sensors*, 2) devices, 3) machines[26].

- IoT Gateway Function: the important gateways are: *RFID, Zigbee, Wi-Fi, 3G/ 4G/ 5G, WAN, LAN, ADSL, LTE*[27].
- IoT Connection Protocols: *IPv6 (PMIPv6), IETF, URI, TCP/IP, UDP, OCF, XS, M2M, SCADA, WSN*[28].
- IoT Services: *energy management, smart home and smart city, place/agent/human monitoring, information shearing between things or systems, value added services for business and manufactures, online media services, agricultures and manufacture process, healthcare, andetc.*

1.1.2. Deterministic IoTApplication

In this research IoT application is referred to the services on the mobile agents. In these applications we have many functions for connection between agents. The details of this distinct application are:

- IoT Infrastructure:
  - **Network**: internetconnection.
  - **Identifier**: the proxy mobile IP for any mobile agents determine a fixed IP number.
  - **Energy**: the mobile agents have their energy and the other equipment amd resources.
- IoT Thigs: mobile agents are as well as smart agents for the internet of things (IoT).
- IoT Gateway Function: the mobile device gateway may be: *Wi-Fi, 3G, 4G, 5G, LAN, ADSL andLTE*.
- IoT Connection Protocols: We define connection protocol base onPMIPv6.
- IoT Services: the mobile device may be support of different applications as well as: smart home applications, smart city applications, data shearing between two or more mobile devices, value added services for business and manufactures, online media services, agricultures and manufacture process, healthcare, andetc.

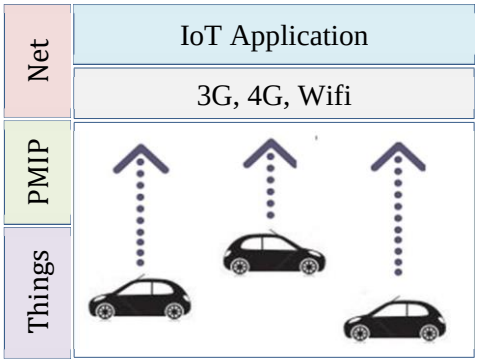


Figure 2. IoT Mobile Agents

1.2. Cloud Computing (CC)Platform

Cloud computing is a new approach for gathering ubiquitous, convenient, on-demand network access as internet where can share pool of IT resources (server, storage, network, application and service). In the cloud network we have scales applications by maximizing concurrency and using computing resources more efficiently one must optimize locking duration, statelessness, sharing pooled resources such as task threads and network connections bus, cache reference data and partition large databases for scaling services to a large number of users [30]. According of NIST definition, we have three models for CC services: *Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS)* that briefly is called SPI model. At the present, the researchers have defined and developed new applicable models of CC that they can be in the one of these three models (Table1).

Table 1. CC Models

SPI models	Applicable models
SaaS	Identity as a Service (IdaaS)
PaaS	Security as a Service (SecaaS), Compliance as a Service (CmaaS)
IaaS	Network as a Service (NaaS), Storage as a service (STaaS), Mobile backend as a service (MBaaS)

Cloud computing (CC) as a new outlook of IT resources and applications, have different methods for design, develop, deploy and launch of services and networks. The CC technology has been emerged based on data sharing and resource distribution as the two mainly cloud paradigms.

In the last five years, data center architecture has been redesigned and migrated to cloud centers architecture as a new generation of IT systems. A cloud center may be deployed as 1) private cloud, 2) public cloud, 3) community cloud and 4) hybrid cloud with specific configuration. The canonical advantages of this new type of computing related to five characters where can list as*: 1) On-demand self-service, 2) Broad network access, 3) Resource pooling, 4) Rapid elasticity, 5) Measuredservice*.

The cloud users have different condition against traditional definition of clients in the server network model. This subject when is more clear to known purpose of cloud computing is to collect distributed resources and provide infrastructure and services so the roles of user in creating, updating, and keeping of IT resource has been eliminated. In Cloud user only has get the control of her/his resources safely [20]. Therefore cloud computing has making the processing capacity and the resource flexibility with high performance for users [21] such that scalability and availability are increased[22].

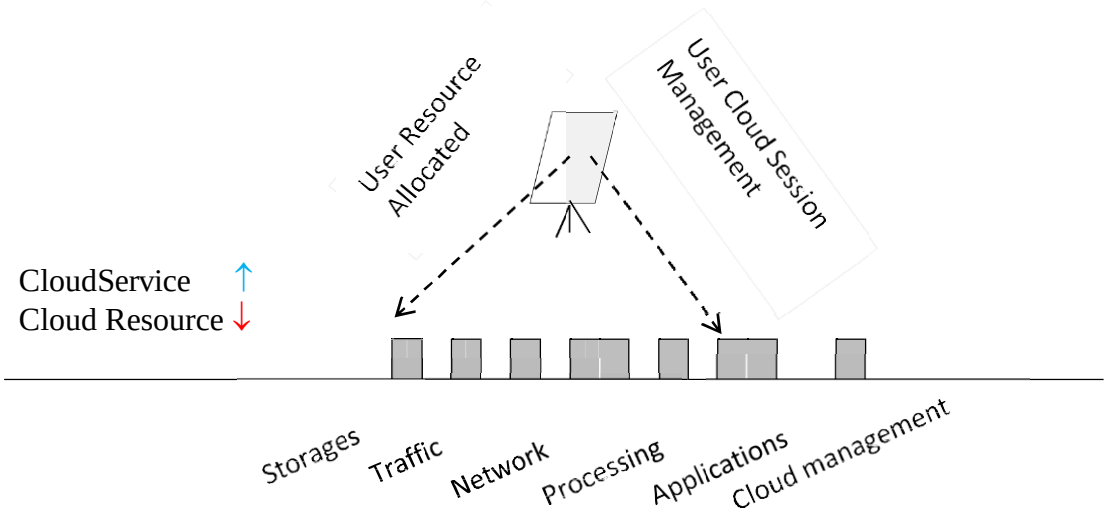


Figure 3. User facilities and flexibility in the cloud centers

Virtual machines (VMs) have provided images of physical machines, which reside in different parts of networks. When allocate some resource of VM to new user/agent VM start a root node for manage its running process (Figure 3).

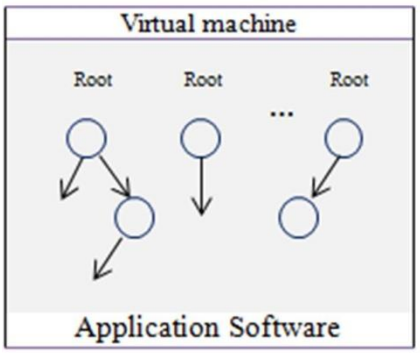


Figure 4. Virtual Machine

The cloud manager follow different services such rate response besides increasing utility of virtual machine and other resource. Anyway a cloud network should be able to provide services for Users/Agents based on service level agreements (SLA) that increase profits ofnetworks.

- **CloudArchitecture**

Point of user view, a data center is an integrated system where provide integrated service. In fact, a data center is consisting of homogeneous or heterogeneous physical machine.

When received many connection from multiple users/agents, data center manager allocate tasks to virtual machines and physical data center has significant effects on performance.

Now, we present architecture of the cloud network based on its components. Cloud architecture consists of several physical machines at different geographical locations over the internet so as to serve the customers optimally. IaaS cloud should support of dynamically coordinating load-shredding among different data centers to determine optimal location for hosting application services. Moreover, cloud service providers may cannot predict geographic distribution of users consuming their services. Therefore, load coordination must happen automatically, and distribution of services must change responding to the changes in load behavior. The following figure depicts service-oriented Cloud Computing architecture consisting of service customer's brokering and provider's coordinator services supporting utility-driven internetworking of clouds.

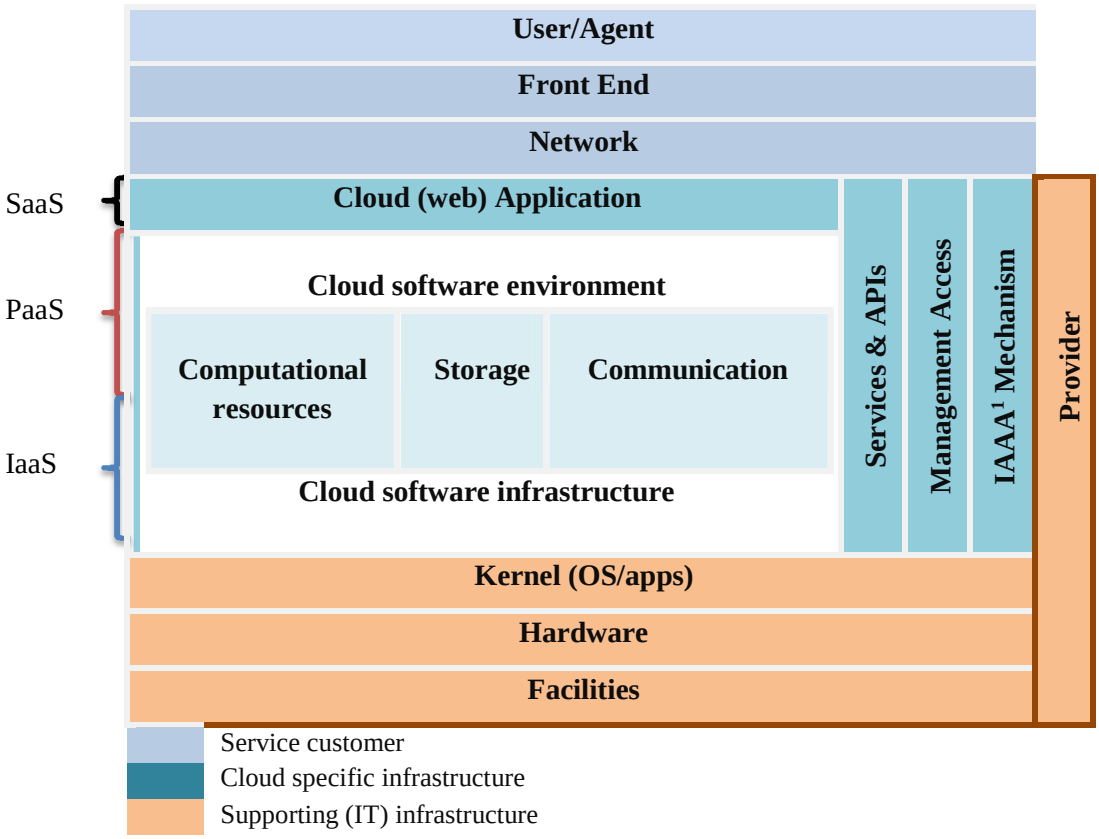


Figure 5. Cloud Architecture

Every data center that (i) exports the cloud services, both infrastructure and platform-level, to the federation; (ii) keeps track of load on the data center and undertakes negotiation with other cloud providers for dynamic scaling of services across multiple

[1] IAAA = Identity, Authentication, Authorization and Auditing

data centers for handling the peak in demands; and (iii) monitors the application execution and over oversees that agreed SLAs are delivered, represents theCloud coordinatorcomponent.

1.3. IoT and Cloud Aggregation

In this research we have decide to review some configuration and ways that may deployed for install IoT service protocols as well as be connected or integrated to a cloud network (Figure 6). Internet of things referred to as connected devices and smart devices where it can to integrate with SaaS layers of cloud networks or convergence with the IaaS cloud conformation. In this chapter we are going to provide an overview of the all methods that IoT and cloud technology for convergent together. Next we interest to IoT–Cloud convergence aspects that are going in particular to analysis the security and resilience challenges.

1.3.1. IoT service: SaaS Integrated or IaaSConnected

Underrevise

1.3.2. Cloud Connection or NetworkConnection

Underrevise

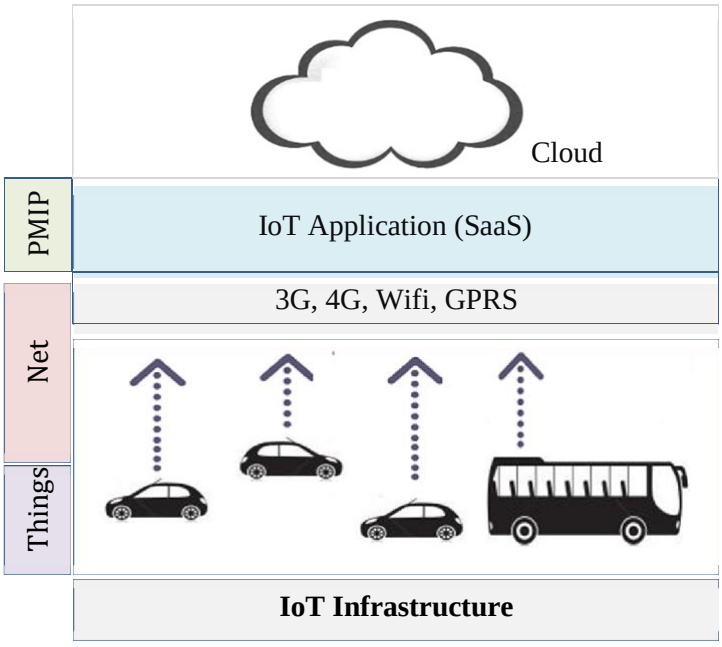


Figure 6. IoT and Cloud

1.4. Security challenges

We have review of advanced security challenges of CC and IoT where have best configuration for aggregation as well as discuss in 1.3 section. If we have three district

parts 1) IoT service and 2) cloud platform and 3) interconnection protocol, then we can to start the investigation of security solutions that may be activated or may be doing progress. We have setup a testbed to measure the performance of network and security overhead.

In this study we will continue the security gaps and security parameters or functions. When a smart device is in the integration architecture or in the connected architecture, at IoT environment, decide to talk with the others (for example share private data), need to be identify firstly, next should be authenticate and audit. In the other side it is necessary to have preventive policy for data protection, information privacy and detection of intrusion behavioral of [8, 9, 12, 14]. For example; if VM A, have a session with VM B, the one of the other VM for example C should be don't have to get information about this secure session. We know security in the cloud has more problems and for a connected service; integrated or connected, the security problems will be increased. For example: security of IoT service when we have network connectivity and we have VMs live migration is harder thanbefore.

Fundamentally, the security of IoT contains three layers: perception layer, transportation layer and application layer. My research will be focused on application layer however we will be considered its correlation with the two other layers. We try to find new solution for our security aspect of IoT service where has specific configuration. In this section we are studying PMIPv6 protocol, for integrated with cloud platform [10, 11, 15], and also try to have been connected to Open Stack platforms and under KVM hypervisor. Open Stack platform deployment is including the Horizon, Nova, Cinder, Glance and Keystone cloud components with a hypervisor selection from KVM, VMware, hyper-V or Xen in deployment in real condition of equipmentnetwork.
In this research we have faced to the three types of security challenges:

IoT and cloud integration threats:

- *Security aspect of integration of IoT and cloud computing in: connection protocols, unify the encryption algorithms and key management systems, provide two-sided identify and mechanizm for accept agents and deliveryservices.*
- *Threat of data breaches in cloud environment and IoTsystem*

Cloud security aspect:

- *Threat of service delivery of cloud for response to the mobile IoTagents*
- *Threat of cloud platform as a centralized server of data andservices*
- *Hypervisor analysis for prevention of introsion and detect of adversaryusers*

IoT security challenges:

- *Condition for secure transaction of IoTagents*
- *Mobile security of*
- *IoTMiddleware*

These security issues of cloud computing are impending for its widespread adoption and managed the IoT services. So, control of user or things, data and applications under these assumptions for an IoT service in a cloud platform is more sophisticate. In this research thesis we have decide to follow security methods for an IoT service when has managed (integrated or connected) in a cloud environment. Now, our work should be addressed in the two aspects;

- **Data**: Proposed a new method for cloud data protection and data confidentiality consist of advanced key-exchange and packetsencryption.
- **Configuration**: Study a secure configuration for an IoT service when is hosted in the cloud platform. For aspect of data shearing inter IoT agent and cloud virtual machine, which has high degree of securityparameters.

We have emphasis on secure architectures for CCIoT connectivity of cloud and IoT service as key management and unify the different cryptographic protocols. Cloud computing architecture on a infrastructure has been supported of both the data storage and the data processing in the outside of the IoT device. In the other side, IoT service support of telecommunication between these device (things, objects, agents) where are smart or only hasmanaged.

2. Problem Statement

Review Internet of Things (IoT) Services, Review
Cloud Computing (CC) Platforms,
Security Solutions for IoT Services under Cloud Platforms.

In this section we have write the details of problem statement where is followed up in thisresearch. We are followed three parts: 1) A specific IoT service and its configuration, 2) distinct cloud platform (the Open Stack platform), 3) Security parameters analysis and try for progress security level and functionality.

This work is including some parts for proposed a new security solution for IoT services where may be considered as the SaaS cloud (as well) or where are services that integrated with IaaS cloud (is well) framework [1, 2, 3, 4, 7, 13]. Therefore we have two approaches for IoT and cloud aggregation that applied to some services. Thus, we can significantly improve deploy or develop the one of advanced solutions for security configuration of connected or integrated IoT and cloud framework. We have a selection from cloud side implementation among Open Stack cloud package and VMware solution and etc. [7, 13], also for IoT service development we are some protocols where are related to applications (smart home, telemedicine, mobile services and etc.) [16, 17, 18], and may be selected. Technically, we have three works for define a security solution for selected IoT services under clouding network.

2.1. CC IoT configuration

The cloud computing (CC) with the more virtual machines (VMs) compared to the physical machines, increase the capability of response to the requests and the throughput of service delivery.

- Firstly we have virtualization as well as under clouding level, where expanded resources by divide the physical resources into multiple VMs with hardware and software partitioning, and time-sharing for resource allocated toVMs.
- Secondly, these expanded resources where are allocated under virtualization has been considered as cloud resources where they will be managed by cloud platform and specificmodules.
- Thirdly, we can to define an IoT service as well as a service of cloud or a service where attained to the cloud. The CC has capacities for provision and support of ubiquitous connectivity and real-time applications and services on smart devices. So, convergence between cloud computing and IoT has become considered as framework for activate the IoTservices.

Figure 1- IoT and Cloud relation

At continue, we present the architecture of the CC with its components and elements when we have an IoT service integrated/connected to the cloud, so we called this CCIoT architecture. Assume that a cloud computing service is consisted of several agents where is consider as "m" virtual machine (m>1). The cycle of agent reception in the cloud system is explained by figure7.

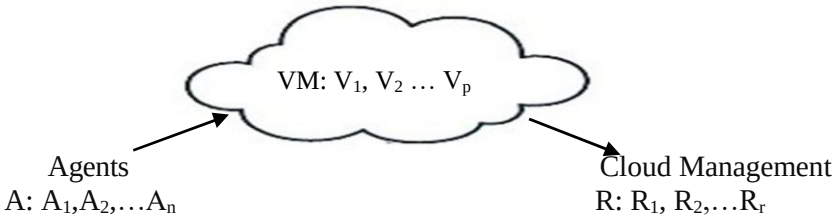


Figure 7. CCIoT cycle

If "A" is the list of agents connected to the cloud, A = {A_1, A_2, …A_m} including "m" numbers of IoT mobile agents, then "A" always changes dynamically on VM. Therefore, in the time of "i", the characteristics of the agent's connected are A_i = {A_{1i}, A_{i2}, …A_{im}}. If resources of R (network, processor, hard space and storages) are obvious R = { R_1, R_2, …R_n}, virtualization to the required number of V_i, are allocated on physical resources. An appropriate solution of "R" is consisting of allocation V_is to agents list. Other words, by R_i as an snapshot in the time "i", the appropriate response of allocation of VMs is provided. Therefore, the set of S ={ R_1, R_2, …R_r } indicates the series of VMs allocate to agents. Figure 7, shows the activity cycle of the cloud. The series of V= {V_1, V_2, …, V_p} shows the number of virtual machines(VM).

Some examples include the limitations of storage, communication capabilities, energy and processing. Such inefficiencies motivate us to connect the technology of Cloud Computing (CC) and the Internet ofThings.

Here, provide a cloud-based connection of agents and IoT-based interconnection for agents such that, can to find a secure solution of R_i agent reception.

.

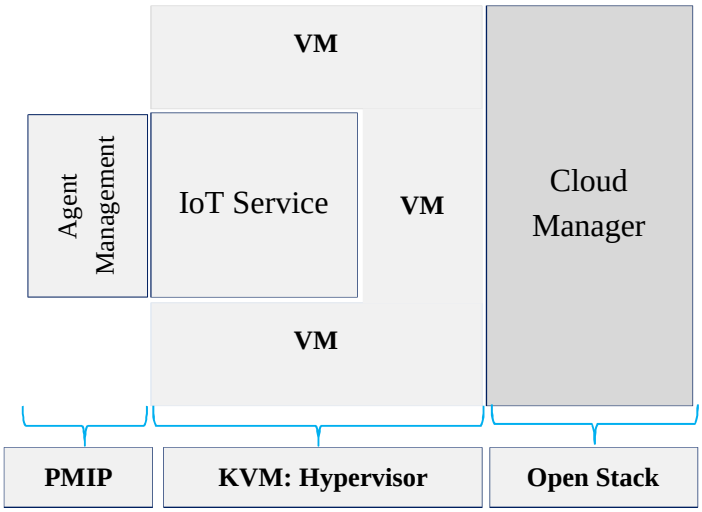


Figure 8. Agent reception in cloud

The intensive computations and the mass storage, which are supported by clouds, are often inefficient. So we more need to deploy a combination model for IoT application and Cloud services. So, cloud computing help us to integrate multiple technologies for maximizing capacity and performance of the existing infrastructure [24].

- **2.1.1. Cloud of Things**
- Under investigate…
- **2.1.2. SLA for CCIoT**
- Under investigate…

2.2.1. Secure Architecture for CCIoT

When 2 or more smart devices (or machines) are connected to a network, from the cloud network perspective they are two or more virtual machines where has been talk with the others and talk with the server. So, it is more different from security discussion where 1) we can to integrated IoT service with an IaaS Cloud platform or 2) we can to get an IoT service as the software as a services (SaaS) cloud, naturally. Now, we try to determine which one is best configuration of IoT service from security aspects.

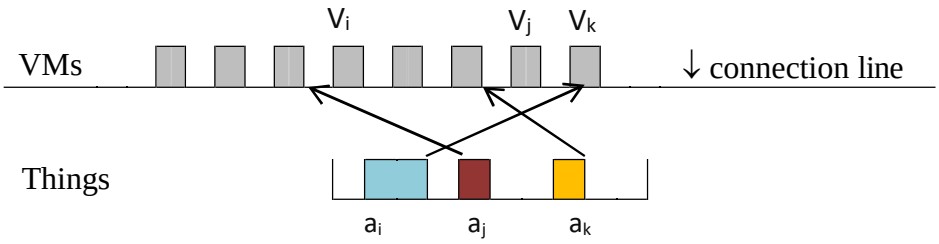


Figure 9. Cloud base connection

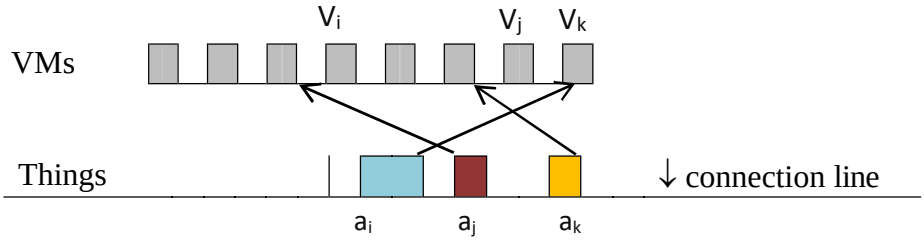


Figure 10. Network base connection

Let u_i and u_j are respectively i and j th of agents where status of them in the correspond virtual machine (VM) V_i and V_j, each agents in the implementation of virtual machine V_i can be found below. Here p_i and q_i are respectively the beginning and end of the session reception an agents on the cloud resources. Thus, the status of each task in the implementation of virtual machine V_i can be found.

2.2.2. Key Management in CCIoT Environment

Integration of Cloud and IoT for a common services with different protocols is required an advanced key management for secure connection of Openstack as cloud platform and PMIP as IoT Service. For CCIoT the security of transfer data across or between cloud and IoT without another party being necessary. Transferred information is accompanied by data encrypted and decrypted and using keys in the send and received packets. So the data encrypted and decrypted should be managed by key lifecycle managers (KLMs) which communicate using a standardized protocol. When we have a cloud services our ideal solution is to allow the users to encrypt all data that is processed or residing in a cloud to avoid unauthorized access. However in CCIoT we have smart agents and cloud users together, and so it is necessary that crypto material have to be managed efficientlyto

reduce risk of security threats. Therefore we need to develop a key management solution where are capable at many functions such as generation, deployment, monitoring, expiration destruction of keys, and et cetera. We have many standardized protocol such as *key management interoperability protocol* (KMIP), which arises due to the proliferation of multiple kinds of cryptographic systems. Now we investigate about KMIP for CCIoT environment and determine some necessary functionality for it. This KMIP will be providing a standard of communication between key management systems and encryption systems to ensure that multiple kinds of systems can be handled using a single Key Management system.

- **PMIPv6 Key Management**
- **Keystone Key Management**

At OpenStack Summit Portland in April 2013, consensus was built around the need to maintain key management as a separate service in its own git repository, incubating the project before finally including it in OpenStack. Specific design criteria established for the key manager included the following[31]:

- **Provide a RESTful API** to create, save, retrieve, and destroy keys, with support for both symmetric and asymmetric keys, and keys of different length
- **Integrate with OpenStack** for authentication and access control
- **Provide audit logging** of key accesses and life cycle events
- **Support high availability** for the key-management service

- **KMIP for CCIoT**

  When we have a KMIP in CCIoT environment we have a standard workflow as bellow:

  1) A key client (User/Agent) makes their request through the API using a client-specific representation.
  2) Then key is encoded in a KMIP format and sent to the server side.
  3) At the server side, the request is decoded using a KMIP decoder to an intermediate representation which is used by the server APIs top rocess.

  KMIP message is encoded in a TTLV format consist of tag, type, length value and etc. KMIP messages are nested, that is the data within the message can be another KMIP message.

<table>
<tr><th>Tag</th><th>Type</th><th>Length</th><th>Value</th></tr>
<tr><td>Attribute</td><td>Structu re</td><td><varie</td><td>
<table>
<tr><th>Tag</th><th>Type</th><th>Length</th><th>Value</th></tr>
<tr><td>Attribute Name</td><td>Structure</td><td><varies></td><td>Application specific ID</td></tr>
<tr><td>Attribute Index</td><td>Integer</td><td>7</td><td>2</td></tr>
<tr><td>Attribute Value</td><td>Structure</td><td><varies></td><td>
<table>
<tr><th>Tag</th><th>Type</th><th>Length</th><th>Value</th></tr>
<tr><td>App Name</td><td>String</td><td><varies></td><td>"ssl"</td></tr>
<tr><td>App ID</td><td>String</td><td><varies></td><td>"domain"</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

Figure 11. TTLV Format of KMIP

For example at bellow we have a sample in the TTLV format where is computed by KMIP system.

Get Unique Identifier

	Operation	02	4	0000000A	Unique Identifier	07	11	*1f165065-ctbd-4bd6-9867-80e0b390ec19*

In this research, we investigate an advanced KMIP where has keep more security of data and connection between agent/user and CCIoT services. Such this protocol will be support of:

- Standardizing communication between encryption systems of IoT part and Cloud part in the CCIoT services.
- Support legacy and new encryption applications.
- Support symmetric keys, asymmetric keys, digital certificates, and other shared secrets process.
- Offer templates for developer that simplify the development and use of KMIP- enabled applications, from encryption client and key-management server.
- Vendors will deliver KMIP-enabled encryption applications that support communication with compatible KMIP key-management servers.

KMIP operation is dividing to three parts: protocol operation, managed objects, and objects attributes. These operations are shown in the Fig 2 and may be increase with the new functions such that provide a proliferation of multiple kinds of cryptographic systems in IoT components or cloud sections.

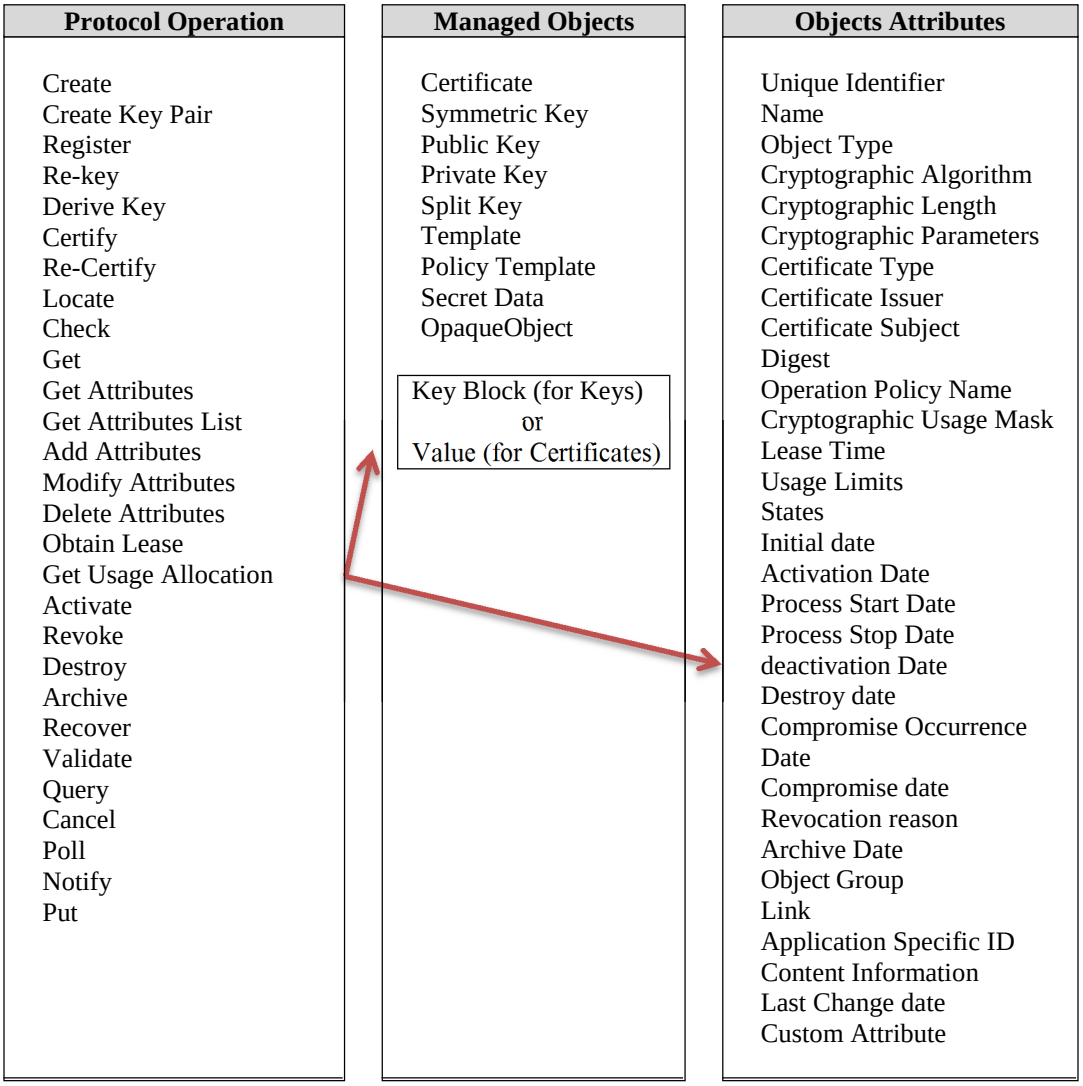


Figure 12. KMIP Protocol operations

❖ **Berbican solution for KMIP in the CCIoT**

Berbican is a open source key management system for Openstack where has a ReSTful API used for generating, storing, deploying and managing of keys which are used for encrypting data handled by different components of Openstack. This solution support of symmetric keys lifecycle management and provides multiple back ends, such as HSM (Hardware Security Modules). Moreover, Dog tag that allow you to configure how to protect the keys, support for the KMIP protocol, allowing it to interface with an external Key Lifecycle Manager server to store and retrieve keys.

PyKMIP is the part of Berbican for develops KMIP where is a Python client which supports key management using the standardized KMIP protocol (Figure 13).

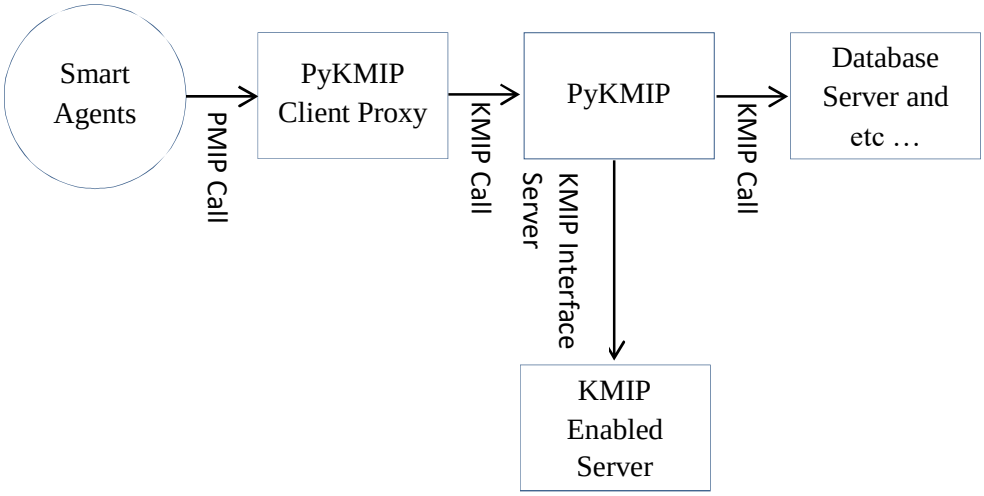


Figure 13. Berbican KMIP solution for CCIoT

This solution provides the capability to connect the client to an external Key Lifecycle Management server which communicates using KMIP protocol. Also, PyKMIP ses a proxy which redirects calls made in Python to a call based on the KMIP protocol which is then forwarded to the appropriate backend based on the configuration.

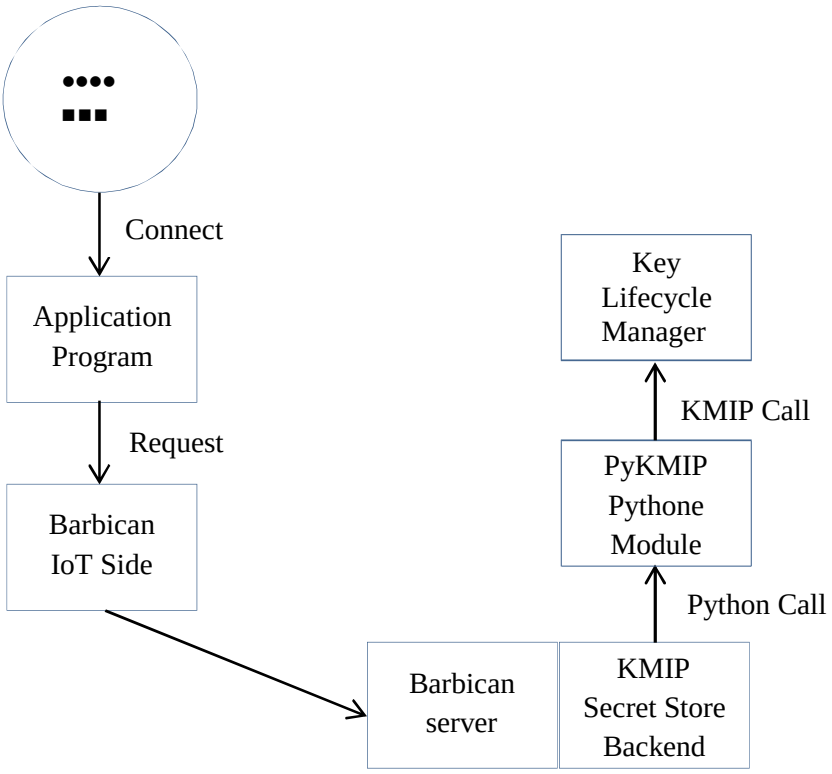


Figure 14. Call follow in PyKMIP

References

[1] Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, **Secure integration of IoT and Cloud Computing**, *Future Generation Computer Systems*,2016.

[2] Alessio Botta, Walter de Donato, Valerio Persico, Antonio Pescap, **Integration of Cloud Computing and Internet of Things: a Survey**, *Journal of Future Generation Computer Systems*, September 18,2015.

[3] Fei Tao, Ying Cheng, Li Da Xu, Lin Zhang, and Bo Hu Li, **CCIoT-CMfg: Cloud Computing and Internet of Things-Based Cloud Manufacturing Service System**, *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 2, May2014.

[4] Lihong Jiang, Li Da Xu, Senior Member, IEEE, Hongming Cai, Zuhai Jiang, Fenglin Bu, and Boyi Xu, **An IoT-Oriented Data Storage Framework in Cloud Computing Platform**, *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 2, May2014.

[5] Chengen Wang, Zhuming Bi, and Li Da Xu, **IoT and Cloud Computing in Automation of Assembly Modeling Systems**, *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 2, May2014.

[6] Enji Sun, Xingkai Zhang, Zhongxue Li, **The internet of things (IOT) and cloud computing (CC) based tailings dam monitoring and pre-alarm system in mines**, *Safety Science* 50 (2012)811–815.

[7] JohnSoldatos,NikosKefalakis,ManfredHauswirth,MartinSerrano,Jean-PaulCalbimonte,MehdiRiahi,Karl Aberer, Prem Prakash Jayaraman, Arkady Zaslavsky, Ivana Podnar Žarko5, Lea Skorin-Kapov, and Reinhard Herzog, **OpenIoT: Open Source Internet-of-Things in the Cloud**, LNCS 9001, pp. 13–25, 2015.

[8] Md. Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan, **Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things**,2015

[9] Qi Jing • Athanasios V. Vasilakos • Jiafu Wan • Jingwei Lu • Dechao Qiu, **Security of the Internet of Things: perspectives and challenges**, *Wireless Netw*,2014.

[10] Aymen Abdullah Alsaffar, Mohammad Aazam and Eui-Nam Huh, **Framework of N-Screen Services based on PVR Micro Data Center and PMIPv6 in Cloud Computing**, *ICUFN*, pp. 839-840,2015

[11] Abdelkader Aissioui, Adlen Ksentini, Abdelhak Gueroui, **PMIPv6-based Follow Me Cloud**, *978-1-4799-5952-5/15/$31.00*, IEEE2015.

[12] Abdullah Gani, Golam Mokatder Nayeem, Muhammad Shiraz, Mehdi Sookhak, Md Whaiduzzaman, Suleman Khan, **A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing**, *Journal of Network and Computer Applications*, 43 (2014)84–102.

[13] Alessio Botta, Walter de Donato, Valerio Persico, Antonio Pescap´e, **On the Integration of Cloud Computing and Internet of Things**, *University of Napoli Federico II*,2014.

[14] Mohammad Aazam, Eui-Nam Huh, **Fog Computing and Smart Gateway Based Communication for Cloud of Things**, *International Conference on Future Internet of Things and Cloud*,2014.

[15] Solomon Emirie Kassahun, Atinkut Astatikie Demissie, **A PMIPv6 Approach to Maintain Network Connectivity during VM Live Migration over the Internet**, *Master Thesis Electrical Engineering*, School of Computing, Blekinge Institute of Technology, Karlskrona, Sweden, October2013

[16] George Suciu, Alexandru Vulpe, Simona Halunga, Octavian Fratu, Gyorgy Todoran, Victor Suciu, **Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things**, *19th International Conference on Control Systems and Computer Science*,2013.

[17] Moataz Soliman, Tobi Abiodun, Tarek Hamouda, Jiehan Zhou, Chung-Horng Lung, **Smart Home: Integrating Internet of Things with Web Services and Cloud Computing**, *IEEE International Conference on Cloud Computing Technology and Science*.2013.

[18] Xiao Ming Zhang, Ning Zhang, **An Open Secure and Flexible Platform Based on Internet of Things and Cloud Computing for Ambient Aiding Living and Telemedicine**, *International Conference on Computer and Management (CAMAN)*, 2011.