Internet of Things and Cloud Computing

Carlos Dores[1], Luís Paulo Reis[1,2,3], Nuno Vasco Lopes[1,2,4]

[1]DSI/EEUM – Departamento de Sistemas de Informação, Escola de Engenharia, Universidade do Minho, Guimarães, Portugal

[2]Centro ALGORITMI, Universidade do Minho, Guimarães, Portugal

[3]LIACC – Laboratório de Inteligência Artificial e Ciência de Computadores, Portugal

[4]Department of Informatics, CISUC R&D Center, University of Coimbra, Coimbra, Portugal

dores.carlos@gmail.com, lpreis@dsi.uminho.pt, nvlopes@dei.uc.pt

Abstract – **With advances in communication technology, future internet presents numerous opportunities to develop new systems designed to make day to day life easier and to enhance and prolong the life of people with disabilities. This motivation propels the development of new services that integrate the mobility of cloud systems and the diversity of IoT (Internet of Things). It will enable us to create new and more independent care systems for people with disabilities, enabling a certain degree of independence. This can have a psychological and social impact due to the better quality of life that enables. Other motivation is the versatility and mobility of services it can provide, making those services available. In this paper is explored and explained the different kinds of technologies that can be integrated to enable creation of future internet platforms. Also, an IoT Cloud platform will be analyzed and some tests will be made, ending with some conclusions and lessons learned in this work.**

Index Terms – IoT, Cloud computing, NGN's, BSN, Disabled People.~

I. INTRODUCTION

With the ever-evolving technologies in computing and communication is important to explore integration of different areas of work with one another. Such is the case of wireless networks, cloud computing and IoT. By integrating these different concepts we may achieve means to deploy systems that can facilitate services that enable or at least improve the quality of people's life. However there isn't any finished platform that integrates these technologies. IoT and Cloud Computing are future internet tendencies, however, IoT technology is based on diversity and not interoperability. Cloud Computing services are dependent on service providers so interoperability and mobility of services between them, is also an issue. In this paper it will be explored a platform that integrates IoT and Cloud technology.

This work will be beneficial to better understand, requirements when creating IoT Cloud systems. The rest of paper is organized as follows. Section II will briefly explain the technologies involved in making the future internet a reality and some limitations that need to be overcome. Section III introduces a platform in development for IoT Cloud integration. Section IV some tests to that same platform will be analyzed. Finally application scenarios will be presented, and conclusions made upon the results obtained.

II. STATE OF THE ART

A. Next-generation networks (NGN's)

NGN's are a concept that aims to make network architectures more flexible and help define and introduce new types services with ease. Being all IP packet based networks, it enables deployment of access independent services over converged fixed and mobile networks. They use IMS at its core which provides access independent platform for different kinds of access technologies such as Wi-Fi, Cable, xDSL, GSM, 3G, 4G and fiber. This enables a great adaptability integrating different technologies. Integration of body sensor networks (BSN's) and social networks through a NGN was analyzed in the article of Mari Carmen Domingo, "*A context-aware service architecture for the integration of body sensor networks and social networks through IP multimedia Subsystem*". An architecture in which the authorized members of a social network can monitor real time data from other user's BSN was proposed [1] [2].

B. IP Multimedia subsystem (IMS) architecture

Defined as a standard by 3GPP, the IP Multimedia Subsystem (IMS) architecture is the core of NGN services. IMS supply telecommunications operators with the ability to deploy an all IP based infrastructure, which enable the launch of new multimedia communication services easily, blending data services with telecommunication services. It can offer cost reduction, by means of IP-boosted increase of capacity for classical services, and the enrichment of other service types, by using former communication services with new ones resulting in a great synergy of the system. It brings a new set of services such as multimedia telephony, instant sharing of multimedia content and live streams, and possibly even new emerging technologies [1] [3] [4] [5].

C. Internet of Things (IoT)

IoT consists in interconnected devices “things” and their addressable virtual representation using standard communication protocols. The heterogeneity of “things”, makes interoperability between them a problem that prevents adoption of generic solutions. Furthermore the volume, speed and volatile data from IoT, impose challenges to existent information services. The will to extend the existent internet with objects, interconnected physical devices and their virtual representation has grown in the last years. This is going to enable the creation of a wide brand of services in different domains, such as smart houses, e-health, transportation, logistics and environmental [6] [7] [8].

D. Wireless sensor networks (WSN’s)

Wireless sensor networks (WSN’s) are a large number of small sensing self-powered nodes which detect events, gather information and communicate wirelessly with the purpose of delivering data to their base station. These networks provide endless opportunities, but challenges need to be overcome, such as energy being a limited resource. The ever-evolving effort in miniaturization and research in nanotechnology, are pushing forward the concept of networked tiny distributed sensors and actuators [9] [10].

E. Body Sensor Networks (BSN’s)

Body sensor networks are a set of sensing devices implanted, internally or externally on a person’s body, linked in a network fashion in a manner that enables the exchange and process of information, so they can act upon events or report them. In the last decade there was a surge of growing interest in new devices for monitoring and sensing on the healthcare area. In the treatment of patients with acute diabetes, a device that controls the release of insulin can monitor the blood glucose level. For epilepsy and other debilitating neurologic disorders, there are already on market, implantable brain stimulators. BSN’s can enable the development of new technologies in healthcare as well in other areas. For this to happen some conception problems need to be solved, such as size, cost and compatibility [11] [12] [13].

F. Cloud Computing

This technology allows to rent infrastructure, runtime environments and services in a pay-per-use basis. It can offer different types of solutions based on user’s requirements, such as, scaling an enterprise infrastructure on demand and sizing it according to the business needs. In case of end users, having their data available anytime anywhere from any device that has a connection to the internet. Cloud Computing is an extremely flexible environment for building new systems and application and even integrating additional capacity or new features into existing systems. Although cloud computing have evolved much its use is still limited to only set of services from a provider. The lack of standardization efforts in the past for this technology made difficult move services from one provider to another [14] [15] [16] [17].

III. THE PLATFORM

Skynet a free and open source platform is still in its developing stages of conception, but already took the first steps for being one viable tool in Future Internet.

Its focus is machine-to-machine (M2M) instant messaging communication. Being an open communication network and API for the Internet of things, “*Skynet is a cloud-based MQTT (MQ Telemetry Transport) powered network that scales to meet any needs”* [18].

“*this platform is able to register and networks devices, giving the ability to store, update and exchange information”*[18].

“*It also provides a queriable device directory API for registering and discovering nodes on the network and maintains presence for each device making easy to know which ones are online and offline*” [18].

It permits connections from a web browser or mobile device, sending messages to one or all devices and subscription to messages being sent to or from devices and their sensors. When devices register, they are assigned a unique id along with a security token. This token is required to authenticate a device. The architecture can be represented as the figure below, the Skynet server on the web, connected to a cloud database, mongoDB (database for clouds). Communications with the Server are typically done via tcp html requests. The protocol of communications between IoT devices that do not have internet able capabilities and their access point such as a computer, are left to the developer criteria.

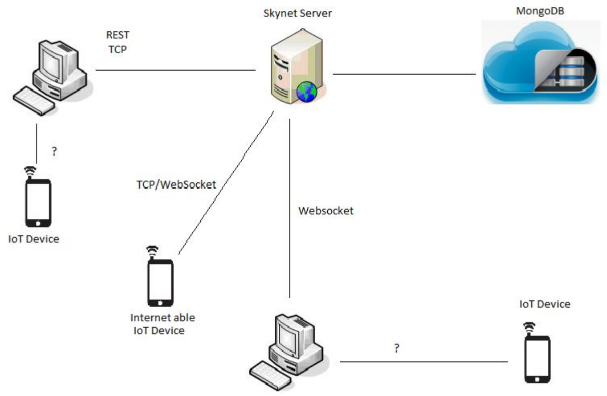


Figure 1 – Skynet Network architecture

IV TESTING THE PROGRAM

Skynet seems a great tool for developing new systems that use IoT and cloud technology. But before we can say that with certainty, some features need to be explored. Features such performance, security, authentication, reliability, quality of service (QoS). To answer these questions tests need to be performed. Because the server didn't allowed ICMP messages, pings couldn't be made to measure the delay. By doing this the server is somewhat protected to DDoS attacks, so it can be seen as a security policy. Simulating pings via tcp, delay times were obtained. The following table of results was calculated based on ten samples, made periodically hour to hour for a period of 24 hours from 11AM of one day to the 10AM of the next day. The time zone standards used where CST (Central Standard Time).

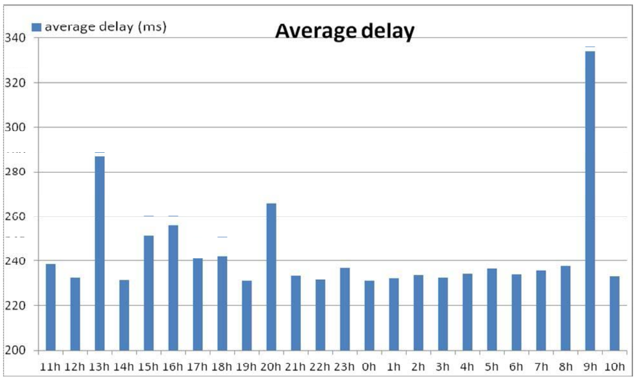


Figure 2 – Delay time results

High Delay is due to Skynet server being located on the West North American continent, so about 200ms (milliseconds) are of RTT (Round Trip Time). The graphic above presents delay times, which are higher during day time when users are awake. The huge spike of delay at 9h corresponds to the start of the working day, when the internet is flooded with requests to services such as e-mail or database requests. The spike at 13h and 20h corresponds to when people leave work and use multimedia and communication services more intensely, such as e-mails, YouTube, Facebook, Skype or gamming services. Analyzing delay times, jitter values were calculated. Jitter is the variation of time between packets arriving; it can be caused by traffic congestion, route changes or time drift. Jitter values were obtained by using the formula:

$$\text{Jitter} = \frac{\text{abs}(T0-T1)+\ldots+\text{abs}(TN-1-TN)}{N-1},\ N=\text{samples}$$

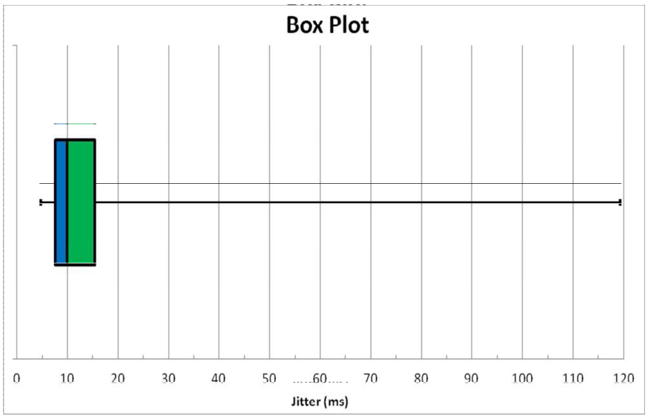
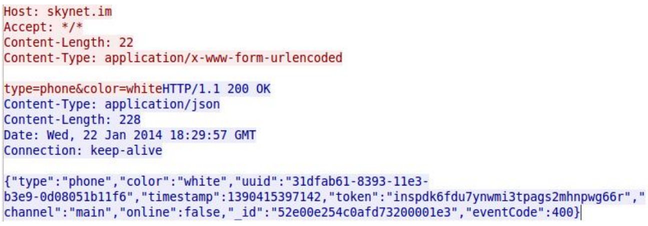


Figure 3 – Jitter Box Plot

Values registered were never lower than 4,76ms and never higher than 119,37ms. Higher values where result of intense activity on the network. The plot above translate that, 25% of values of jitter were between 5 and 9ms, 50% were between 9ms and 15ms and 25% of values were higher than 15ms and lower than 119ms. With high congestion of the network, jitter can be a problem, affecting QoS potentially resulting in inoperability of real-time systems. The security that Skynet provide is, a secret token associated to a unique uuid. The purpose of this token is to ensure that only authorized entities are able to change critical information associated to that same device. Whenever changes to critical information need to be done, the token must be provided. As this is an open communication system, information is not ciphered and senders and receivers are not authenticated via secured connections. This means users are susceptible to man in the middle attacks and information privacy is not ensured, as seen in the following figure.



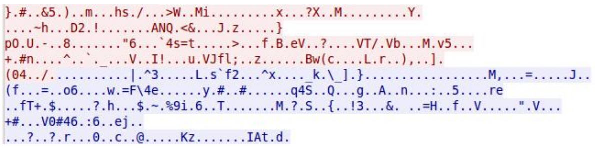
```
Host: skynet.im
Accept: */*
Content-Length: 22
Content-Type: application/x-www-form-urlencoded

type=phone&color=whiteHTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 228
Date: Wed, 22 Jan 2014 18:29:57 GMT
Connection: keep-alive

{"type":"phone","color":"white","uuid":"31dfab61-8393-11e3-
b3e9-0d08051b11f6","timestamp":1390415397142,"token":"inspdk6fdu7ynwmi3tpags2mhnpwg66r","
channel":"main","online":false,"_id":"52e00e254c0afd73200001e3","eventCode":400}
```

Figure 4 – Wireshark token capture test

As we can see the information is visible, even the token that is secret information only the owner should know, can be seen. The token was the security measure in place, and in some scenarios that might be enough. On the other hand this level of security, is not enough in scenarios that unauthorized access to the devices can have catastrophic results and loss of human lives. One of such cases is the use of emergency button for the elderly. If the secret token was intercepted, other entities can in theory use it to send an emergency signal that is authenticated as a user in distress. This failure in privacy can lead to a DDoS like attack, flooding the system with emergency requests, leaving emergency services without means to respond to all requests and unable to tell which ones are real. This means communications like this need to be protected by authentication and ciphering. If this is done, the information exchange should be secure as seen in the figure bellow.



```
}.#..&5.)..m...hs./...>W..Mi.........x...?X..M.........Y.
....~h...D2.!.......ANQ.<&...J.z.....}
pO.U.-..8.......“6...`4s=t.....>...f.B.eV..?....VT/.Vb...M.v5...
+.#n....^..`._...V..I!...u.VJfl;..z......Bw(c....L.r..),..].
(04../...........|.^3.....L.s`f2...^x...._k.\_].}.................M,...=.....J..
(f...=..o6....w.=F\4e......y.#..#......q4S..Q...g..A..n...:..5....re
..fT+.$.....?.h...$.~.%9i.6..T.......M.?.S..{..!3...&. ..=H..f..V.....".V...
+#...V0#46.:6..ej..
...?..?.r...0..c..@.....Kz.......IAt.d.
```

Figure 5 – Wireshark secure communication capture

In this example of a secure communication using an ssl websocket, data is ciphered. Using this method, receiver and sender are authenticated to one another. This however require more processing power. That might be a problem due to the limited processing power and energy reserves of an IoT device. This means that more research needs to be done before we can say which way is best for securing IoT communications.

V Application scenarios

Skynet is an open communications system, so information privacy is not a concern. This means that it can only be used in scenarios that don't require that feature, such as a device that information can be seen and altered by everybody, like an air-conditioner thermostat. In scenarios that require that feature, is not a recommended system. For instance, if the levels of insulin administered by a device to a patient that suffers from diabetes, where to be altered by other than the authorized personal, this could result in death. There are many scenarios that security is a required, and a good level of security is recommended to be used in all systems. As for QoS the platform wouldn't be able to provide a service with real time requirements to users further away, since the server is localized in west United States, the round trip time is to long so the responsiveness of devices is affected. Also Jitter seems to be a big problem when networks have high activity, so a way to overcome that, needs to be explored.

VI Conclusions

IoT and cloud platforms will be a certainty in the future, however more research need to be done. Especially on the privacy and authentication process's that secure communications. Also performance tests to measure the impact of using these security technologies need to be done, because energy consumption is an issue. On the aspect of QoS, service also needs to be improved. Since the distance to users might be long, delay could be a problem. ITU G.114 specification recommends less than 150 millisecond (ms) one-way end-to-end delay for high-quality real-time traffic such as voice, so that requirement need to be. This could be achieved by installing servers closer to users, reducing round-trip time.

Acknowledgments

This work has been partially supported by FCT – Fundação para a Ciência e Tecnologia within the Project Scope: PEst-OE/EEI/UI0027/2014 and PEst-OE/EEI/UI0319/2014.

References

[1] Syed A. Ahson and Mohammad Ilyas, "IP multimedia subsystem (IMS) handbook", 2009 by Taylor & Francis Group.

[2] M. C. Domingos, "A context-aware service architecture for the integration of body sensor networks and social networks through IP multimedia Subsystem", 2011 IEEE Communication Magazine.

[3] Khalid Al-Begain, Chitra Balakrishna, Luis Angel Galindo and David Moro, "IMS: A Development and Deployment Perspective", 2009 John Wiley & Sons Ltd.

[4] G. Camarillo and M. A. García-Martín, "The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds", 2004 Wiley.

[5] 3GPP Tech. Spec., "IP Multimedia Subsystem (IMS) (Release 7)," 2006; http://www.3gpp.org/ftp/Specs/html-info/23228.htm.

[6] Payam Barnaghi, Wei Wang, Cory Henson and Kerry Taylor, "Semantics for the Internet of Things: early progress and back to the future", http://personal.ee.surrey.ac.uk/Personal/P.Barnaghi/doc/IJSWIS_SemIoT_CR_2.pdf.

[7] Rajkumar Buyyab, Jayavardhana Gubbia, Slaven Marusica and Marimuthu Palaniswamia, "Internet of Things (IoT): A vision, architectural elements, and future directions", February 2013 Elsevier Inc.

[8] Mari Carmen Domingo, "An overview of the Internet of Things for people with disabilities", in Journal of Network and Computer Applications, vol. 35 (2012) 584–596, Domingo, 2012.

[9] Martin Haenggi and Daniele Puccinelli, "Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing", Third Quarter 2005, IEEE Circuits and Systems Magazine.

[10] P. Fergus et al. "A Framework for Physical Health Improvement using Wireless Sensor Networks and Gaming", Proc. Pervasive Health '09, Apr. 2009.

[11] Benny P L Lo, Guang-Zhong Yang, "Key Technical challenges and current implementations of Body sensor networks", http://vip.doc.ic.ac.uk/bsn/public/UbiMonPapers/Key_Technical_Challenges_and_Current_Implementations_of_Body_Sensor_Networks.pdf.

[12] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Commun., vol. 17, no. 1, Feb. 2010, pp. 51–58.

[13] M. Patel and J. Wang, "Applications, Challenges, and Prospective in Emerging Body Area Networking Technologies," IEEE Wireless Commun., vol. 17, no. 1, Feb. 2010, pp. 80–88.

[14] Rajkumar Buyya, Christian Vecchiola and S. Thamarai Selvi, "Mastering Cloud Computing Foundations and Applications Programming", 2013 Elsevier Inc.

[15] Dan C. Marinescu, "Cloud Computing Theory and Practice", 2013 Elsevier Inc.

[16] Ileana Castrillo, Derrick Rountree and Hai Jiang as Technical Editor, "The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice", 2013 Elsevier Inc.

[17] Randee Adams and Eric Bauer, "Reliability and availability of cloud computing", 2012 by IEEE, http://www.buyya.com/papers/SensorWeb2010Chapter20.pdf.

[18] Skynet, available online at: http://skynet.im/ [consulted on Feb 2014]